The Innovation of Social Studies Journal
Vol. 7, (2), March 2026: 280-291
ISSN: 2716-2354 (p); 2723-1119 (e) DOI: https://doi.org/10.20527/iis

Public Value Creation Through QRIS Use In Bojonegoro: A Public Service Dominant Logic Approach

Keyka Wahyu Putri Octavia[1], Muhammad Miftahul Huda[2], Sri Kasiami[3]

[1] Faculty of Social and Political Sciences, Universitas Bojonegoro; keykaputri2004@gmail.com
[2] Faculty of Social and Political Sciences, Universitas Bojonegoro; miftahjatim@gmail.com
[3] Faculty of Social and Political Sciences, Universitas Bojonegoro; sri.kasiami@gmail.com

ARTICLE INFO

Keywords:

QRIS; Public Value; Transaction Security; PSDL; Digital Public Service.

Article history:

Received 25-12-29
Revised 26-01-13
Accepted 26-01-01
Published 2026-03-01

ABSTRACT

Digital transformation has expanded digital public services, including retail payment systems through the Quick Response Code Indonesian Standard (QRIS). Despite its rapid adoption and benefits in improving transaction efficiency and convenience, digital security risks and potential fraud may affect public trust and service sustainability. This study aims to examine perceptions of security and the process of public value creation in the use of QRIS in Bojonegoro Regency, as well as the role of institutions in ensuring the security and sustainability of QRIS as a digital public service. This study employs a qualitative approach using in-depth interviews with users, culinary merchants, regulators (Bank Indonesia), and payment service providers (PSPs). Data were thematically analyzed using the public value concept and the Public Service-Dominant Logic (PSDL) framework. The findings indicate that QRIS is positively perceived in terms of convenience and efficiency; however, perceptions of security and transaction certainty remain varied. Fraud risks and transaction failures encourage users and merchants to adopt precautionary practices, highlighting the importance of institutional responsiveness in maintaining public trust. The study demonstrates that public value in QRIS is co-created through interactions among actors, technology, and service experiences, positioning transaction security as a key factor for the sustainability of digital payment services at the local level.

Corresponding Author:
Keyka Wahyu Putri Octavia
Faculty of Social and Political Sciences, Universitas Bojonegoro; keykaputri2004@gmail.com

1. INTRODUCTION

Digital transformation has encouraged governments to expand innovation in digital public services, including within the retail payments sector. Payment digitalization is positioned as a policy instrument to enhance efficiency, inclusiveness, and transparency in public services. However, the accelerated adoption of digital services also brings new challenges, particularly related to transaction security, fraud risks, and the sustainability of public trust in service-providing institutions. In the context of the national payment system, Bank Indonesia (BI) responded to the need for efficiency and financial inclusion by launching the Quick Response Code Indonesian Standard (QRIS) in 2019 as a national standard for QR code–based payments (Bank Indonesia, 2025).

The growth in QRIS usage demonstrates a significant acceleration in everyday economic activities. This trend is consistent with findings indicating that perceived ease of use and security are key predictors of QRIS adoption across various regions in Indonesia (Jundy Kumoro et al., 2024). Such growth is reflected in InterActive QRIS operational data, which show that by 2025 QRIS had reached 57 million users and 39.3 million merchants, with a transaction volume of 6.1 billion and a transaction value of IDR 317 trillion recorded in the second quarter of 2025 (InterActive QRIS, 2025). To observe long-term acceleration, data from the Indonesian Payment System Association (ASPI), published via Databoks, indicate a consistent upward trend in both the volume and value of QRIS transactions from 2021 through the second quarter of 2025, signaling the increasing integration of QRIS across various economic sectors and service activities.

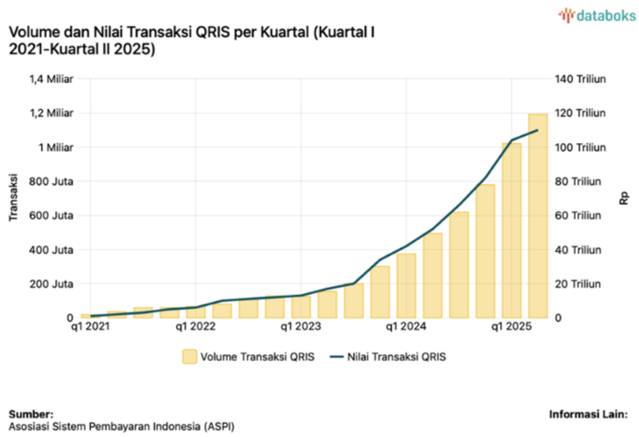

Figure 1. QRIS Transaction Volume and Value per Quarter (First Quarter of 2021-Second Quarter of 2025).
Source : Asosiasi Sistem Pembayaran Indonesia (ASPI) as reported by Databoks (2025).

However, this rapid growth has been accompanied by heightened digital security risks. Various QR-based crime schemes, such as sticker swapping and QR phishing, have become more prevalent in public spaces. Users who are concerned about security tend to perceive risk as a significant barrier to the adoption of digital payment systems, as they associate such technologies with the potential misuse of personal data or unauthorized transactions (Nabila et al., 2025). In addition, a study by Ardianto (2025) emphasizes that the success of QRIS is strongly influenced by users' ability to understand transaction-related risks as well as the clarity of the regulator's role in ensuring the security of the digital payment system.

The increasing security risks in digital payment services are reflected not only in fraudulent practices but also in users' perceptions of transaction outcome uncertainty and data protection. Empirical studies indicate that perceived transaction risk and system security significantly influence users' acceptance of QRIS services, particularly when users do not fully understand the available protection mechanisms and risk management processes (Pulungan et al., 2025). Furthermore, trust in the providing institutions has been shown to play a crucial role in shaping the sustainability of QRIS usage, especially among younger users, where confidence in institutional protection and risk mitigation mechanisms strengthens long-term usage intentions (Fikri et al., 2025). The growing prevalence of phishing and digital security risks has also been examined in the academic literature, which emphasizes the importance of security literacy and internal control practices in preventing fraud in digital payment services (Azmi et al., 2024; Kartika & Machmuddah, 2026).

In the context of digital payment systems, the literature further emphasizes that technological innovation cannot be separated from the strengthening of governance and institutional oversight. Gomber et al. (2017) argue that, in the absence of adequate regulatory frameworks, digital payment innovations may increase systemic risks that can disrupt service stability and erode public trust. Therefore, the role of government and regulatory authorities becomes a critical element in ensuring that digital payment systems develop in a secure and sustainable manner.

Government and regulatory support for digital payment systems such as QRIS has been reported to strengthen user trust and support long-term adoption (Puspitasari & Salehudin, 2022). Academic literature indicates that the clarity of regulatory frameworks, adequate consumer protection, and consistent institutional governance play a significant role in building trust and legitimacy in digital payment services, particularly within the context of fintech-based innovation (Arner et al., 2017; Claessens et al., 2018). In this context, the strengthening of payment system governance should not be understood merely as the establishment of technical rules, but rather as an institutional process whose effectiveness must be empirically examined through everyday usage practices at the local level to ensure that security and consumer protection are genuinely perceived by users and business actors Zetzsche et al. (2020).

Bojonegoro Regency provides a relevant context for examining the dynamics of QRIS adoption as a digital payment service, given its strong reliance on micro, small, and medium enterprises (MSMEs) and locally driven economic activities. Empirical studies indicate that MSMEs in developing regions are increasingly shifting from cash-based transactions to digital payments due to their perceived practicality, efficiency, and ability to support more systematic financial record-keeping (Suryono et al., 2020). Beyond usability factors, the literature emphasizes that government support, facilitation programs, and improvements in digital financial literacy play a critical role in strengthening trust and ensuring the sustainability of digital payment adoption at the local level (Rahayu & Day, 2017). From the governance perspective, field findings highlight an end-to-end governance approach that integrates policy design, technical implementation, and user behavior change to expand the benefits of QRIS while maintaining security, reliability, and legal compliance.

Conceptually, this study positions Public Value as the primary foundation for assessing the substantive value generated by QRIS, including the prerequisites for sustainability through the dimensions of legitimacy and public support as well as the operational capacity of service providers (Moore, 1995). Within this framework, Public Service-Dominant Logic (PSDL) is used as an analytical approach to examine how public value is formed through actor interactions, service exchanges, resource integration, and institutional arrangements within the service ecosystem, thereby enabling a more detailed explanation of co-creation processes and service experiences (Osborne et al., 2013; Vargo & Lusch, 2004, 2016).

Much of the existing research on QRIS and digital payments has primarily focused on quantitative measurements related to *intention to use, continuance use*, or the effects of trust and transaction security on user behavior. While these approaches provide important insights into the factors influencing technology adoption, they tend to fall short in capturing the dynamics of service experience and the processes of public value creation in the practical use of QRIS as a digital public service. Lember et al. (2019) argue that digital technologies have the potential to transform the relationship between the state and citizens through processes of public value creation and service co-creation; however, they also emphasize the need for context-specific, local-level studies to understand these dynamics in greater depth.

Based on this research gap, this article aims to analyze the creation of public value in the use of QRIS as a digital public service in Bojonegoro Regency. Specifically, the study seeks to address two research questions: (1) how are perceptions and processes of public value creation in QRIS use shaped by digital transaction security and fraud risks among community members and culinary-sector businesses in Bojonegoro; and (2) what roles do institutions particularly Bank Indonesia, payment service providers (PSPs), and merchants play in ensuring the security and sustainability of QRIS as a digital public service.

2. METHODS

This study employs a qualitative approach to analyze the experiences and perceptions of actors involved in the use of QRIS as a digital public service at the local level. A qualitative approach was chosen to capture the dynamics of transaction security and fraud risks within their natural context, without the intention of testing hypotheses or statistically examining relationships between variables (Creswell, 2018). The focus of the study is directed toward the gap between the high rate of QRIS adoption and the potential security risks and sustainability challenges of digital payment services as a form of public service.

The research was conducted in Bojonegoro Regency and involved 8 informants who are key actors in the QRIS ecosystem, including 1 representative from Bank Indonesia, as the regulator Mr. Imam Solihin, 2 PSPs (Bank BRI, Mr. Alfin, and Bank BNI, Mr. Fatoni), 3 merchants (2 coffee shop attendants, namely Ms. Vira and Ms. Hafiza, and Ms. Riska as the owner of a small business), and 2 users, Mr. Zainal Ali and Mr. Ardi Sufrian. Informants were selected using purposive sampling based on their direct involvement in the use, management, and oversight of QRIS. This approach was employed to ensure a diversity of perspectives and sufficient depth of information to adequately understand the phenomenon of digital public services at the local level (Palinkas et al., 2015).

Data were collected through in-depth interviews and a review of policy documents related to the payment system. Data analysis was conducted thematically through processes of coding, categorization, and interpretation, guided by the Public Service-Dominant Logic framework and the concept of public value. Data credibility was ensured through source triangulation and member checking, whereby interview findings were reviewed to ensure consistency and trustworthiness (Lincoln & Guba, 1985).

3. FINDINGS AND DISCUSSION

The use of QRIS as a digital public service in Bojonegoro Regency is perceived positively in terms of transaction convenience and efficiency. However, perceptions regarding security and fraud risks remain ambivalent, especially among merchants in the culinary sector. These findings were obtained from in-depth interviews with users, merchants, regulators, and payment service providers, which were then analyzed thematically using the concept of public value and the Public Service-Dominant Logic (PSDL) framework.

3.1. Perceptions of Users, Merchants, PSPs, and Bank Indonesia regarding QRIS Transaction Security

The findings indicate that users' and culinary business actors' perceptions of QRIS transaction security in Bojonegoro Regency vary considerably. On the one hand, QRIS is perceived as a practical, fast, and convenient payment system that facilitates daily transactions. On the other hand, both users and merchants continue to express concerns regarding potential fraud and the validity of digital transaction evidence.

For culinary business actors, the use of QRIS is considered operationally beneficial, particularly during peak business hours. Hafiza, a cashier at a coffee shop, representing merchants, stated that QRIS simplifies transactions because it eliminates the need to prepare change and is more practical overall. She emphasized that QRIS payments are faster during busy periods, noting that *"using QRIS is quicker, especially when it's crowded, so it's not complicated by having to prepare change"* (interview, merchant, 2025). This statement suggests that, from a functional perspective, QRIS is perceived as an efficient payment system that supports service continuity.

Nevertheless, field findings also reveal that this sense of security is not yet fully established. Merchants remain concerned about the possibility of transaction evidence manipulation, such as edited screenshots or transactions that appear successful but where funds are not actually received. Vira, a cashier at another coffee shop, stated that she *"does not feel completely secure yet because QRIS fraud is not always visible, and transaction photo evidence can be edited"* (interview, merchant, 2025). These concerns lead merchants to conduct additional manual checks, such as matching transaction notifications, reviewing payment histories, or asking customers to show proof of payment. This practice indicates that perceptions of QRIS security do not rely solely on the system, but are still strongly influenced by individual vigilance.

A similar perspective was expressed by Riska, a merchant, who acknowledged that QRIS facilitates transactions and accelerates service delivery. Nevertheless, she still feels the need to conduct additional checks on incoming transactions. Such caution is considered necessary to ensure that payments are successfully completed and funds are actually received, particularly during peak business hours (interview, merchant, 2025).

These findings suggest that, for merchants, QRIS security is primarily perceived as a functional prerequisite that supports smooth business operations, especially in high-transaction situations. Within the public value framework Moore (1995), this condition reflects that the value of security remains at an instrumental level as a means to enhance service efficiency rather than having fully evolved into a substantive public value grounded in trust. The persistence of manual verification practices indicates that system legitimacy has not yet fully replaced the role of individual vigilance in everyday practice.

In contrast, QRIS users generally perceive the system as secure as long as transactions are conducted through official applications and the payment destination matches the merchant's name. One user, Ardi Sufarian, explained that before making a payment, he always verifies the transaction destination by *"double-checking the merchant's name, because as far as I know, store names cannot be duplicated"* (interview, user, 2025). This statement indicates that users' sense of security is largely constructed through personal vigilance rather than through a technical understanding of QRIS security mechanisms.

Another user, Zainal Ali expressed a similar view, stating that while QRIS makes daily transactions. However, a sense of security still depends on users' habits of verifying payment destinations and keeping transaction records. These experiences suggest that trust in QRIS is built through personal precautionary practices rather than solely through confidence in the technical system itself (interview, user, 2025).

From the users' perspective, security in QRIS usage is largely shaped by personal caution rather than by an understanding of the system's technical security mechanisms. This finding reinforces the view that in digital public services, trust does not automatically emerge from technological design, but rather develops through repeated experiences that users perceive as consistent and predictable. In terms of public value, this indicates that security is still individually constructed and has not yet been fully internalized as collective trust in the digital payment system.

Taken together, findings from both users and merchants demonstrate that perceptions of QRIS security are shaped by practical, everyday experiences rather than by confidence in system design or institutional guarantees alone. Manual verification practices by merchants and careful payment confirmation by users indicate that a sense of security has not yet been fully attached to QRIS as a system that is automatically trusted. This condition reflects that trust in digital payment services remains situational and dependent on individual practices, with security perceived as something that must be continuously ensured rather than as an established guarantee.

Overall, interview findings suggest that QRIS security, from the perspectives of users and merchants, is not understood as an absolute guarantee provided by the system, but rather as the outcome of a combination of system reliability and user vigilance. Within the public value framework, transaction security constitutes a crucial dimension of public value, as it is directly related to safety, trust, and the legitimacy of digital public services. When a sense of security is not fully established, the public value generated by QRIS tends to remain functional limited to convenience and efficiency rather than fully developing into a substantive public value supported by strong trust.

From the perspective of banking PSPs, QRIS security is understood as the result of system strengthening and institutional readiness in handling complaints. An informant from BRI, Alfin, explained that QRIS systems are fundamentally designed with adequate security standards; however, vigilance from users and merchants remains necessary to minimize potential fraud, such as falsified transaction evidence or incorrect payment destinations. In addition, banks provide customer service channels for complaints in case transaction issues arise, with the aim of ensuring that problems are addressed promptly and public trust in QRIS services is maintained (interview, PSP–BRI, 2025).

From another PSP perspective, QRIS is viewed as a payment system that is inherently secure because it operates under the standards and supervision of Bank Indonesia, although operational risks are still acknowledged as possible. Security is understood to depend not only on technical systems, but also on complaint-handling mechanisms and user vigilance. Fatoni emphasized that issues such as transaction failures can be resolved through formal bank complaint procedures, while data security is maintained through internal monitoring and coordination with relevant authorities. Therefore, user literacy and caution are regarded as important factors in sustaining trust and the long-term viability of QRIS services (interview, PSP–BNI, 2025).

Overall, the perspectives of banking payment service providers indicate that QRIS security is perceived as the outcome of a combination of system reliability, institutional readiness in handling complaints, and the level of user literacy and vigilance. Although QRIS has been designed with robust security standards and operates under the supervision of Bank Indonesia, operational risks are acknowledged as part of the dynamics of digital payment systems. Consequently, responsive complaint mechanisms and user education are considered essential elements in maintaining public trust and sustaining the adoption of QRIS as a digital payment service.

From the regulator's perspective, views on QRIS security emphasize a different dimension. Bank Indonesia perceives security as the result of layered system design and standardized regulation. An informant from Bank Indonesia, Imam, explained that from the outset, QRIS was designed using a comprehensive governance approach, ranging from technical standard-setting to user education, with the objective of ensuring broad benefits while keeping risks under control. He emphasized that *"the objective of QRIS is clear, in line with its CEMUMUAH slogan (Fast, Easy, Affordable, Secure, and Reliable), and one QR code for all applications. It is intended to deliver broad and inclusive benefits, while risks must remain controlled"* (interview, BI informant, 2025). This statement indicates that from the regulator's perspective, security is understood as an institutional attribute that is systematically designed and maintained.

These differing perspectives among actors reveal a gap between institutionally designed and maintained security, as perceived by regulators and PSPs, and empirically experienced security among users and merchants in everyday practice. Within the public value framework, this condition suggests that the value of security has not yet been fully internalized as comprehensive public trust. From a PSDL perspective, this divergence underscores that security value is not determined solely by system design, but also by service experiences encountered by actors in practice. Security value is therefore the result of a co-creation process involving institutions, technology, and everyday usage practices, which remains dynamic and not yet fully stabilized as collective trust.

Accordingly, the first research question is addressed at the perceptual level: QRIS security is understood in layered ways by users, merchants, and institutional actors, with positive assessments regarding convenience and service efficiency, yet persistent doubts regarding transaction certainty. As a result, the public value generated remains primarily functional and has not yet been fully institutionalized as public trust.

3.2. Fraud Risk and Precautionary Practices in QRIS Use

In the literature on digital payment services, security risks are not limited to fraud but also include service breakdowns and uncertainty in transaction outcomes, which can shape users' trust and perceived security (Grönroos, 2011; Rafaeli et al., 2017). This perspective positions security as a construct that is not purely technical, but also related to the service experience and certainty of results felt by users and merchants. Consistent with this view, the present study finds that both behavioral risks and system-related disruptions contribute to precautionary practices among users and merchants.

At the merchant level, prominent concerns relate to falsified proof of payment and discrepancies in payment status. In busy conditions, merchants noted that potential errors or fraud may be harder to detect immediately. These concerns have prompted informal precautionary measures such as verifying notifications, cross-checking transaction histories, and requesting additional confirmation before finalizing an order.

A further risk involves transaction failure. Although not necessarily categorized as fraud, transaction failure significantly affects perceived security. One user described an incident in which a friend's payment was deducted from the account balance, yet the transaction was recorded as failed: *"it had been paid, the money had been deducted, but the transaction failed"* (User interview, 2025). Such incidents create uncertainty because funds are deducted while completion is delayed, requiring follow-up through complaint channels. This suggests that transaction failures can generate insecurity comparable to fraud, particularly when outcomes are not immediately verifiable.

At the user level, awareness of these potential risks has led to the emergence of various forms of personal caution. Users tend to double-check merchant names, ensure that the applications they use are official, and save transaction receipts in case of problems. Double-checking has become the main mechanism used by users to minimize risk, as well as a form of adaptation to the limited information they have about the technical aspects of the QRIS security system.

From the PSP perspective, the risk of fraud and transaction failures is understood as part of the dynamics of the service that must be managed through complaint handling and rapid response mechanisms. Informants from the bank emphasized that although the QRIS system is considered secure, users and merchants still need to remain vigilant. *"Banks provide customer service as a channel for complaints to handle transaction problems, with the main objective of maintaining public trust so that it does not decline when transaction disruptions or errors occur"* (PSP interview, 2025).

Within a public value framework, fraud risk and transaction failure can erode the value generated by QRIS if not managed effectively. Conversely, user and merchant precautions, coupled with responsive institutional handling by PSPs, serve as buffer mechanisms that help sustain public trust. Through a PSDL lens, these precautionary practices illustrate value co-creation: users and merchants act as active participants who adapt behavior to maintain service quality and reduce risk, while institutions support the ecosystem through operational systems and dispute-resolution mechanisms.

Thus, the first research question is addressed from a risk perspective, indicating that QRIS security is not perceived solely in terms of the absence of fraud. Security is also understood through transaction certainty and the responsiveness in handling transaction disruptions. These factors directly shape users' sense of safety and their trust in QRIS as a digital public service.

3.3. The Role of Bank Indonesia and PSPs in Maintaining QRIS Security and Sustainability

The findings indicate that the sustainability and security of QRIS as a digital public service are not determined solely by technological quality. Instead, they depend heavily on the institutional roles of Bank Indonesia and Payment Service Providers (PSPs) in maintaining and reinforcing public trust through everyday service practices. In this context, security and sustainability are experienced by users and merchants as ongoing processes that require policy consistency, operational readiness, and the ability of institutions to respond effectively to risks and service disruptions at the field level.

From a regulatory perspective, Bank Indonesia plays a strategic role in ensuring that QRIS functions as a secure, reliable, and inclusive payment system. Informants from Bank Indonesia explained that QRIS security is designed as a layered system, encompassing technical standards, transaction limits, and continuous education for both users and merchants. From the regulator's viewpoint, service sustainability is closely linked to system stability and risk minimization without compromising ease of use, which reinforces QRIS legitimacy through public communication and digital literacy initiatives.

However, empirical findings from merchants suggest that regulatory safeguards do not automatically translate into a fully secure service experience. Several merchants expressed that their trust in QRIS security remains conditional, particularly due to concerns about unstable internet connections and the possibility of manipulated transaction proof. This indicates a gap between institutionally designed security and the security perceived in everyday transactional practices.

In this context, banking PSPs occupy a crucial position as the direct operational interface between the QRIS system and its users. Field findings indicate that PSPs interpret service security not only as a system attribute, but also as institutional readiness to manage complaints and transaction disruptions. Informants from PSPs emphasized that customer service channels function as the primary mechanism for resolving transaction failures and suspected fraud, making responsiveness a key factor in sustaining trust.

User and merchant experiences show that interactions with PSP customer service strongly shape long-term perceptions of QRIS security. When complaints are handled in a responsive and transparent manner, perceived risks tend to decrease even when service disruptions occur. Conversely, delays or unclear problem-handling processes may amplify uncertainty and erode the public value generated through service convenience and efficiency.

Within the public value framework, the roles of Bank Indonesia and PSPs can be understood as a collective effort to sustain the legitimacy and public trust of QRIS as a digital public service. As noted by Hajar and Arma (Hajar & Arma 2024), legitimacy in digital public services is shaped through actor involvement and citizens' service experiences. Accordingly, security and sustainability are assessed not only through fraud prevention indicators, but also through institutional presence and responsiveness when problems arise.

Viewed through the lens of Public Service-Dominant Logic (PSDL), QRIS sustainability emerges from continuous interactions among regulators, PSPs, merchants, and users within a service ecosystem. Bank Indonesia provides system-level governance and policy direction, while PSPs operationalize service delivery and manage direct user interactions. Security and sustainability are therefore constructed through value co-creation processes involving multiple actors and everyday usage practices (Blaschke et al., 2019; Rodriguez Müller et al., 2021).

The findings emphasize that the sustainability of QRIS as a digital public service is largely determined by institutional capacity to balance convenience and risk management. Ease of use must be accompanied by adequate security mechanisms and responsive operational practices to maintain public trust. Accordingly, the second research question is addressed by highlighting the complementary institutional roles through which QRIS security and sustainability are collectively maintained over time.

Accordingly, the second research question is addressed by highlighting the complementary institutional roles in maintaining QRIS security and sustainability. Bank Indonesia ensures system standards, stability, and legitimacy, while Payment Service Providers (PSPs) manage service experiences and operational disruptions at the implementation level. The alignment of these roles enables QRIS to sustain its public value over time despite evolving security challenges.

3.4. Theoretical Discussion: Public Value and PSDL in QRIS Digital Payment Services

To synthesize the empirical findings and theoretical insights discussed earlier, this study develops a conceptual model of QRIS security value co-creation as a digital public service. The model is employed to explain how interactions among regulators, service providers, merchants, and users shape public value in the context of QRIS transaction security. Figure 2 presents a visual representation of this co-creation process, positioning security as the outcome of the integration of institutional resources and everyday usage practices at the operational level.

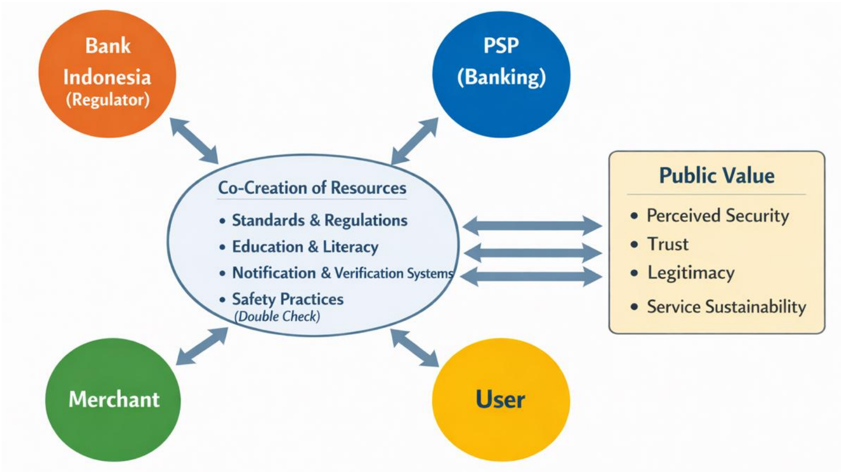

Figure 2. Co-Creation Model of QRIS Security Value as a Digital Public Service
Source: Author's work (2025)

As shown in Figure 2, QRIS security is co-created through the integration of institutional resources such as standards and regulations, education and digital literacy, notification and verification systems, and user precautionary practices. These elements interact dynamically through service encounters between users and merchants, supported by institutional frameworks provided by regulators and PSPs. The resulting public value manifests in the form of perceived security, trust, legitimacy, and service sustainability.

The empirical findings demonstrate that public value creation in QRIS is not automatic, even when transaction efficiency and convenience are achieved. While ease and speed of transactions function as essential prerequisites, the sustainability of public value is more strongly influenced by security perceptions and transaction certainty. This explains why QRIS generates strong functional value but still faces challenges in transforming this value into stable public trust.

Within the public value framework, these findings reinforce the view that public value extends beyond functional service performance to include legitimacy and citizen trust in implementing institutions. QRIS successfully delivers instrumental public value through efficiency and accessibility; however, inconsistent experiences of transaction security weaken its institutionalization as substantive public value. Consequently, security and certainty of transaction outcomes emerge as critical conditions for strengthening public value in digital payment services.

From a Public Service-Dominant Logic (PSDL) perspective, Figure 2 illustrates that security and trust are co-created rather than unilaterally produced by institutions. Users and merchants actively shape service quality through cautious behaviors such as verifying payment destinations and transaction confirmations. Simultaneously, Bank Indonesia and PSPs enable value co-creation by providing regulatory frameworks, system infrastructure, and complaint-handling mechanisms that sustain service continuity during disruptions.

The model also highlights a gap between institutionally designed security and empirically experienced security. For institutions, security is defined by compliance with technical and regulatory standards, whereas for users and merchants, security is primarily understood as transaction certainty and rapid problem resolution. This divergence underscores that public value creation in digital services depends heavily on the institution's capacity to translate system-level security into tangible service experiences.

Theoretically, these findings confirm that public value is contextual, dynamic, and interaction-based. In the case of QRIS, public value is shaped not only by the presence of digital payment technology but by how security is enacted and experienced in everyday transactions. PSDL provides an explanatory lens to understand how service sustainability relies on continuous resource integration and interaction among actors within an evolving service ecosystem.

Thus, by anchoring the analysis in Figure 2, this study positions transaction security as a central mechanism in the co-creation of public value. QRIS as a digital public service must therefore ensure not only efficiency and inclusiveness, but also that security and risk management are experientially felt by users and merchants. This theoretical synthesis integrates the first and second research questions by demonstrating that QRIS sustainability depends on the alignment between user–merchant perceptions and institutional roles in maintaining a consistent security experience..

4. CONCLUSION

This study concludes that the use of QRIS as a digital public service in Bojonegoro Regency has generated public value, particularly in terms of transaction convenience and efficiency. However, this value has not yet been fully institutionalized, as perceptions of security and transaction certainty remain varied among users and merchants. The findings indicate that security is not perceived solely as the absence of fraud, but also as the assurance that transactions are successfully completed and that disruptions are handled promptly and transparently.

Addressing the first research question, the study finds that risks associated with QRIS usage include both behavioral risks and system-related risks, which directly affect users' sense of security and trust. These risks encourage the emergence of precautionary practices among users and merchants, such as double-checking transactions and retaining proof of payment. Such practices demonstrate that users and merchants act as active participants in maintaining service quality and mitigating risks within the digital payment ecosystem.

In response to the second research question, the sustainability and security of QRIS are maintained through the complementary roles of Bank Indonesia and Payment Service Providers (PSPs). Bank Indonesia functions as the guardian of system standards, regulations, and institutional legitimacy, while PSPs manage service experience and operational-level disruption handling. The interaction among regulators, PSPs, merchants, and users forms a process of value co-creation that determines whether security and public trust in QRIS can be sustained over time.

Theoretically, these findings confirm that public value in digital public services is contextual and dynamic, and highly dependent on the quality of service interactions. Through the lenses of public value and Public Service-Dominant Logic, transaction security emerges as a key element in the co-creation of public value. Accordingly, the sustainability of QRIS is determined not only by technological design, but also by the capacity of the system and its actors to maintain a consistent and trustworthy security experience for the public.

REFERENCES

Ardianto, H. (2025). Peluang dan Tantangan Implementasi Sistem Pembayaran Digital bagi Produktivitas UMKM di Era Ekonomi Digital. *Lokawati: Jurnal Penelitian Manajemen Dan Inovasi Riset*, *3*, 290–302. https://www.researchgate.net/publication/396098748_Peluang_dan_Tantangan_Implementasi_Sistem_Pembayaran_Digital_bagi_Produktivitas_UMKM_di_Era_Ekonomi_Digital

Arner, D. W., Barberis, J., Buckley, R. P., Arner, D., & Barberis, J. (2017). FinTech, RegTech, and the Reconceptualization of Financial Regulation. In *Northwestern Journal of International Law & Business* (Vol. 37, Issue 3). http://scholarlycommons.law.northwestern.edu/njilb/vol37/iss3/2

Azmi, M., Fadillah, A., Ramadhan, M. G., & Ariefiandi, M. E. (2024). Jakarta Raya;Jl. Raya Perjuangan No. 81 Marga Mulya. *Journal of Information and Information Security (JIFORTY)*, *5*(2), 88955882. http://ejurnal.ubharajaya.ac.id/index.php/jiforty

Bank Indonesia. (2025). *Quick Response Code Indonesian Standard (QRIS)*. Bank Indonesia. https://www.bi.go.id/id/fungsi-utama/sistem-pembayaran/ritel/kanal-layanan/qris/default.aspx

Blaschke, M., Riss, U., Haki, K., & Aier, S. (2019). Design Principles for Digital Value Co-creation Networks: a Service-dominant Logic Perspective. *Electronic Markets*, *29*(3), 443–472. https://doi.org/10.1007/s12525-019-00356-9

Claessens, S., Frost, J., Turner, G., & Zhu, F. (2018). Fintech Credit Markets Around the World: Size, Drivers and Policy Issues. *BIS Quarterly Review*.

Creswell, J. D., & Creswell, J. W. (2018). *Research Design Qualitative, Quantitative,and Mixed Methods Approaches (Fifth)*. SAGE.

Databoks. (2025). *Tren Transaksi QRIS Meningkat pada Kuartal I 2025*. https://databoks.katadata.co.id/keuangan/statistik/68931f19ba160/tren-transaksi-qris-meningkat-pada-kuartal-i-2025

Fikri, M., Herlina, L., & Winar, I. (2025). *Pengaruh Kepercayaan dan Persepsi Risiko terhadap Penggunaan QRIS sebagai Instrumen Transaksi Keuangan Digital pada Generasi Z di Kota Bandung*. https://doi.org/10.61104/alz.v3i5.2864

Gomber, P., Koch, J. A., & Siering, M. (2017). Digital Finance and FinTech: current research and future research directions. *Journal of Business Economics*, *87*(5), 537–580. https://doi.org/10.1007/s11573-017-0852-x

Grönroos, C. (2011). A Service Perspective on Business Relationships: The Value Creation, Interaction and Marketing Interface. *Industrial Marketing Management*, *40*(2), 240–247. https://doi.org/10.1016/j.indmarman.2010.06.036

Hajar, S., & Arma, N. A. (2024). Co-creating Public Value Into Digital-Based Public Service Innovation in the Village Governance. *Otoritas : Jurnal Ilmu Pemerintahan*, *14*(3), 516–538. https://doi.org/10.26618/ojip.v14i3.15891

InterActive QRIS. (2025). *Pertumbuhan Transaksi QRIS yang Melonjak Memahami Revolusi Pembayaran Digital di Indonesia*. https://qris.interactive.co.id/homepage/blog-detail.php?lang=id&page=MjEz-pertumbuhan-transaksi-qris-yang-melonjak-memahami-revolusi-pembayaran-digital-di-indonesia

Jundy Kumoro, C., Ryandini, E. Y., & Samin, N. (2024). Faktor-Faktor Yang Mempengaruhi Adopsi Pembayaran QR Code (QRIS) di Toko Fisik. *Journal of Innovation in Management, Accounting and Business*, *3*(2), 97–112. https://doi.org/10.56916/jimab.v3i2.865

Kartika, L. N. I., & Machmuddah, Z. (2026). Gen Z's Understanding Of Internal Controls Dominates Qris Phishing Prevention. *Keuangan Dan Auditing*, *6*(2), 32–46. https://doi.org/10.56696/jaka.v6i2.15318

Lember, V., Brandsen, T., & Tõnurist, P. (2019). The potential Impacts of Digital Technologies on Co-production and Co-creation. *Public Management Review*, *21*(11), 1665–1686. https://doi.org/10.1080/14719037.2019.1619807

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic-Inquiry*. SAGE Publications. Rafaeli, A., Altman, D., Gremler, D. D., Huang, M. H., Grewal, D., Iyer, B., Parasuraman, A., & de Ruyter, K. (2017). The Future of Frontline Research: Invited essays. Journal of Service Research, 20(1),

Moore, M. H. (1995). *Creating Public Value Strategic Management in Government*. Harvard University. https://www.researchgate.net/publication/257496373_Creating_public_value_Strategic_management_in_government_Cambridge_MA_Harvard_University_Press_by_Mark_Moore

Nabila, A. P., Raharso, S., & Tiorida, E. (2025). The Influence of Trust and Transaction Security on Interest in Using The QRIS Payment System. *Airlangga Journal of Innovation Management*, *6*(2), 248–260. https://doi.org/10.20473/ajim.v6i2.72597

Osborne, S. P., Radnor, Z., & Nasi, G. (2013). A New Theory for Public Service Management? Toward a (Public) Service-Dominant Approach. *American Review of Public Administration*, *43*(2), 135–158. https://doi.org/10.1177/0275074012466935

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research. *Administration and Policy in Mental Health and Mental Health Services Research*, *42*(5), 533–544. https://doi.org/10.1007/s10488-013-0528-y

Pulungan, L. H., Pratama, A., & Faroqi, A. (2025). Evaluasi Faktor Penerimaan Pengguna Terhadap Layanan QRIS Pada Generasi Z Menggunakan Modifikasi TAM. *Jurnal Pendidikan Dan Teknologi Indonesia*, *5*(4), 1091–1110. https://doi.org/10.52436/1.jpti.781

Puspitasari, A. A., & Salehudin, I. (2022). Quick Response Indonesian Standard (QRIS): Does Government Support Contribute to Cashless Payment System Long-term Adoption? *Journal of Marketing Innovation (JMI)*, *2*(1). https://doi.org/10.35313/jmi.v2i1.29

Rafaeli, A., Altman, D., Gremler, D. D., Huang, M. H., Grewal, D., Iyer, B., Parasuraman, A., & de Ruyter, K. (2017). The Future of Frontline Research: Invited Commentaries. *Journal of Service Research*, *20*(1), 91–99. https://doi.org/10.1177/1094670516679275

Rahayu, R., & Day, J. (2017). E-commerce adoption by SMEs in developing countries: evidence from Indonesia. *Eurasian Business Review*, *7*(1), 25–41. https://doi.org/10.1007/s40821-016-0044-6

Rodriguez Müller, A. P., Flores, C. C., Albrecht, V., Steen, T., & Crompvoets, J. (2021). A Scoping Review of Empirical Evidence on (Digital) Public Services Co-creation. In *Administrative Sciences* (Vol. 11, Issue 4). MDPI. https://doi.org/10.3390/admsci11040130

Suryono, R. R., Budi, I., & Purwandari, B. (2020). Challenges and Trends of Financial Technology (Fintech): A systematic literature review. In *Information (Switzerland)* (Vol. 11, Issue 12, pp. 1–20). MDPI AG. https://doi.org/10.3390/info11120590

Vargo, S. L., & Lusch, R. F. (2004). Evolving to a New Dominant Logic for Marketing. *The Service-Dominant Logic of Marketing: Dialog, Debate, and Directions*, *November*, 3–28.

Vargo, S. L., & Lusch, R. F. (2016). Institutions and Axioms: an Extension and Update of Service-Dominant Logic. *Journal of the Academy of Marketing Science*, *44*(1), 5–23. https://doi.org/10.1007/s11747-015-0456-3

Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralized Finance. *Journal of Financial Regulation*, *6*(2), 172–203. https://doi.org/10.1093/jfr/fjaa010