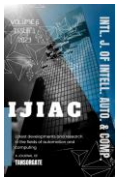


International Journal of Intelligent Automation and Computing

Research Article OPEN ACCESS

Integrating Digital Wallets: Advancements in Contactless Payment Technologies

Shobhit Agrawal
Sr. Staff Software Engineer in Visa Inc
Bothell, WA, USA
https://orcid.org/0009-0000-4957-5575

Abstract

The rapid advancements in digital wallets and contactless payment technologies have transformed the way consumers conduct transactions. This research provides an in-depth analysis of the integration of digital wallets and the progress made in contactless payment technologies, focusing on four key areas: contactless communication technologies, security and authentication measures, device integration, and enhanced functionality. Near Field Communication (NFC) and Quick Response (QR) codes have emerged as the dominant contactless communication technologies that digital wallets to facilitate secure and seamless transactions. The use of QR codes has expanded beyond smartphones, with integration into wearable devices. To safeguard against fraudulent activities, digital wallets employ tokenization and secure element technologies. Tokenization replaces sensitive credit card information with unique tokens, while the secure element provides an isolated environment for token storage. Biometric authentication methods, such as fingerprint scanning, facial recognition, and iris scanning, have been incorporated into digital wallets to verify user identity and authorize transactions. The integration of digital wallets has extended to various devices, including smartwatches, fitness trackers, and smart rings, equipped with NFC technology. Modern point-of-sale (POS) systems have also been upgraded to support NFC and QR code transactions, facilitating seamless acceptance of digital wallet payments by merchants. Digital wallets have evolved to incorporate loyalty programs and rewards systems, allowing users to store loyalty cards, collect points, and redeem rewards directly through their wallets. Efforts towards interoperability and standardization have been made to ensure compatibility and security across different digital wallet providers and payment networks.

Keywords: Authentication, Contactless communication, Device integration, Enhanced functionality, NFC technology, Security measures, Tokenization

Declarations

Competing interests:

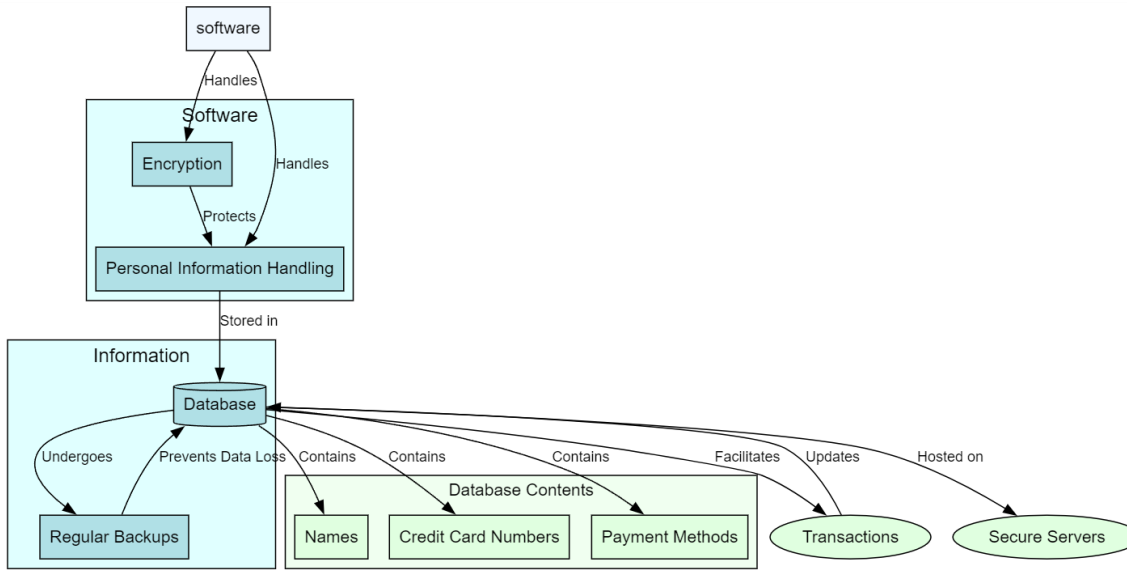
The author declares no competing interests.

Introduction

The "*Digital Revolution"* has brought about significant changes in various aspects of our lives, including the way we conduct financial transactions. The digitization of money has paved the way for the

emergence of digital wallets, which are becoming increasingly popular as a convenient and secure alternative to traditional payment methods [1], [2]. A digital wallet is a digital system that allows users to perform electronic transactions, such as purchasing goods and services, transferring money, and receiving payments, all from a single platform.

Figure 1. The Software and Data Components of Digital Wallets



Digital wallets offer several advantages over traditional payment methods. Firstly, they provide a high level of convenience, as users can access their funds and make transactions from anywhere, at any time, using their mobile devices. This eliminates the need to carry physical cash or credit cards, which can be lost or stolen. Digital wallets often come with built-in security features, such as encryption and two-factor authentication, which help protect users' sensitive information from unauthorized access [3], [4].

Many digital wallets allow users to store ID documents, driver's licenses, loyalty cards, and other important information that would normally be carried in a physical wallet. This centralization of information makes it easier for users to manage their personal data and reduces the risk of losing important documents.

The technology behind digital wallets is comprised of two main components: *software and information*. The software component is responsible for handling users' personal information and ensuring the security of their data through encryption [5], [6]. This encryption helps protect sensitive information from being accessed by unauthorized parties for providing users with peace of mind when using their digital wallets for transactions.

The information component of digital wallets is stored in a database that contains details such as names, credit card numbers, and payment methods. This information is used to facilitate transactions and ensure that funds are transferred accurately and efficiently between parties. The database is typically hosted on secure servers and is regularly backed up to prevent data loss in

the event of a system failure or cyber-attack.

Digital wallets also offer many money transfer techniques in order to make it easy for users to send and receive funds. One popular method is the use of Quick Response (QR) codes, which can be scanned using a smartphone camera to initiate a transaction. Near Field Communication (NFC) allows users to make contactless payments by simply holding their mobile device near a payment terminal. Bluetooth-based transactions are also becoming more common for enabling users to transfer funds wirelessly between devices [7], [8].

Digital wallets eliminate the need to carry physical cash or credit cards by providing a secure, centralized repository for payment information. This streamlined approach to payment management allows for transactions to be executed with just a few taps on a smartphone. This helps reducing the hassle and inconvenience associated with traditional payment methods. Digital wallets alleviate the burden of remembering multiple card numbers, expiration dates, and security codes, as all this critical information is securely stored within the wallet itself.

In addition to their convenience, digital wallets boast a remarkable level of speed and efficiency. Transactions processed through digital wallets are executed almost instantaneously, minimizing the time spent waiting for payment approvals or change to be counted. This expedited transaction process is particularly advantageous for businesses, as it can lead to enhanced customer satisfaction and increased sales volume. Digital wallets streamline the checkout process, both in-store and online, by automatically populating payment and shipping information, thereby reducing the likelihood of errors and abandoned carts.

Digital wallets ensure the protection of users' sensitive financial information by employing advanced encryption and tokenization technologies. When a transaction is initiated using a digital wallet, the actual card numbers are not shared with the merchant. Instead, a unique, single-use code is generated for each transaction, significantly reducing the risk of fraud and unauthorized purchases [9]. Many digital wallets incorporate biometric authentication measures, such as fingerprint or facial recognition, providing an additional layer of security to prevent unauthorized access to the wallet.

The proliferation of contactless payments has further amplified the allure of digital wallets. Equipped with NFC (Near Field Communication) technology, many digital wallets enable users to execute payments by simply holding their smartphone in close proximity to a compatible payment terminal. This contactless payment approach is not only faster and more convenient than traditional card payments but also more hygienic, as it minimizes the need for physical contact with payment devices. The demand for contactless payments has experienced a significant surge, catalyzing the widespread adoption of digital wallets on a global scale.

Through partnerships with retailers, airlines, and other businesses, many digital wallet providers offer exclusive discounts, cashback incentives, and loyalty points to users who utilize their wallets for payments. These rewards can be effortlessly tracked and redeemed within the wallet app, offering a seamless and convenient way for users to save money and enjoy additional perks.

For those who frequently engage in online shopping, digital wallets have become an indispensable tool. Digital wallets significantly simplify the online checkout process by securely storing payment and shipping information within the wallet. Users are no longer required to input their card details and address for each individual purchase for reducing the risk of typing errors and the time spent completing transactions. This convenience has resulted in increased conversion rates for online merchants and an improved overall shopping experience for customers.

Digital wallets have also greatly facilitated the management of international payments and currencies. When traveling abroad, users can effortlessly convert funds to the local currency within their digital wallet, eliminating the need to carry substantial amounts of cash or visit a currency exchange. Some digital wallets even allow users to hold multiple currencies simultaneously, simplifying the process of managing expenses while traveling and avoiding unnecessary conversion fees.

Digital wallets assist users in tracking their spending and managing their budgets more effectively. The majority of digital wallet apps come equipped with built-in expense tracking and categorization features, providing users with understandings into their spending habits. This information can be utilized to create budgets, set financial goals, and make informed decisions regarding future purchases. Users can identify areas where they may be overspending and take proactive steps to curb unnecessary expenses by having a clear overview of their finances.

One concern is the risk of cyber-attacks and data breaches, which could compromise users' personal and financial information. While digital wallet providers invest heavily in security measures, no system is completely foolproof, and users must remain vigilant in protecting their data. Another issue is the potential for technical glitches and system failures, which could prevent users from accessing their funds or completing transactions. This can be problematic in emergency situations where immediate access to funds is necessary. Not all merchants and service providers accept digital wallet payments, which can limit their usability in certain situations.

There are also concerns about the impact of digital wallets on personal privacy. As more personal information is stored in digital form, there is a risk that this data could be misused or exploited by third parties. Digital wallet providers must be transparent about their data collection and usage practices and give users control over how their information is shared and used. The adoption of digital wallets, however, continues to grow rapidly, driven by the increasing popularity of e-commerce and the desire for more convenient and secure payment options.

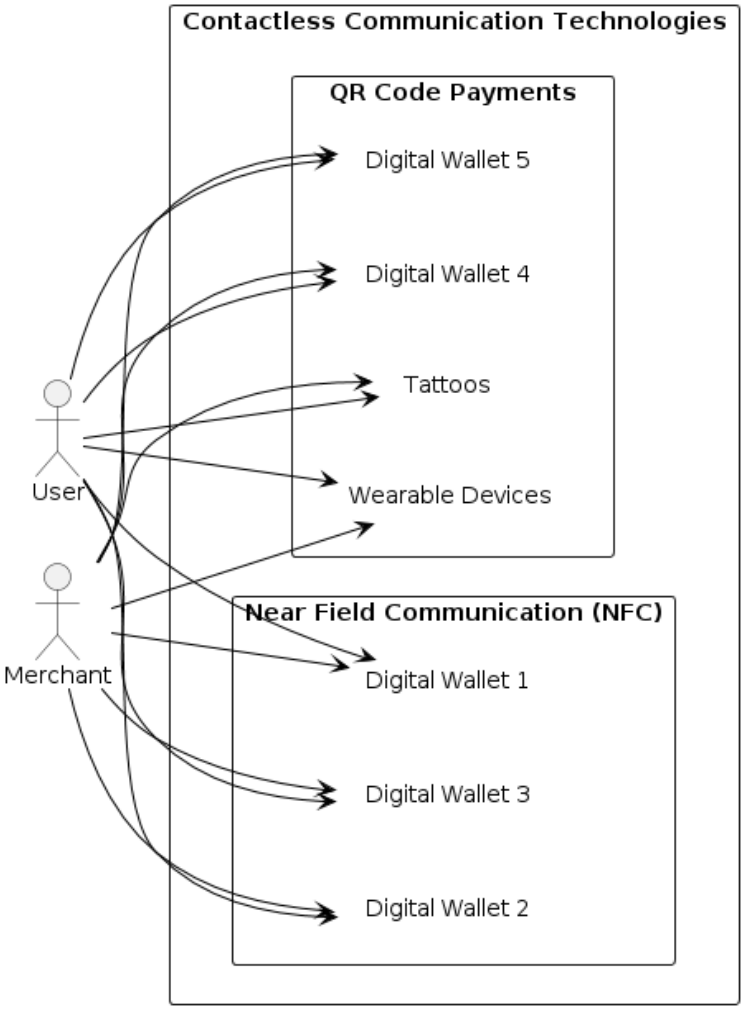
Contactless Communication Technologies

1. Near Field Communication (NFC):

Near Field Communication (NFC) is a short-range wireless technology that allows devices to communicate with each other when they are in close proximity, typically within a few centimeters. It enables convenient data exchange between devices, such as smartphones, tablets, and wearable gadgets, by simply bringing them close together [10], [11]. NFC operates on the principle of electromagnetic induction, where data is transferred between devices via radio waves. The technology consists of three primary components: *the initiator,*

the target, and the carrier frequency. The initiator device generates an RF field that powers the target device and enables communication. The target device responds to the initiator's signal, exchanging data as necessary.

Figure 2. Contactless Communication Technologies in Digital Wallets



NFC technology enables contactless transactions by allowing devices to communicate wirelessly when in close proximity. Digital wallets like Apple Pay, Google Pay, and Samsung Pay use NFC to facilitate secure and seamless transactions. Users can simply tap their smartphone or smartwatch on an NFC-enabled payment terminal to complete a transaction.

2. QR Code Payments:

Quick Response (QR) codes are two-dimensional barcodes that store information in a machine-readable format. They consist of black squares arranged on a white background, often with a square border around them [12]–[14]. QR codes can store various types of data, such as text, URLs, contact information, or other forms of structured data. The primary components of a QR code include the finder pattern, the timing pattern, and the

alignment pattern. The finder pattern helps scanning devices locate and orient the QR code, while the timing pattern assists in determining the size and position of the individual modules within the code. The alignment pattern ensures accurate scanning by providing reference points for adjusting the scanning angle [15], [16].

Quick Response (QR) codes have gained popularity as a contactless payment method. Digital wallets allow users to scan QR codes displayed by merchants to initiate payments. This technology has expanded beyond smartphones, with QR codes being integrated into wearable devices.

Security and Authentication:

1. Tokenization and Secure Element:

Tokenization is a security process that replaces sensitive data, such as credit card numbers or personal identification numbers (PINs), with unique identification symbols called tokens. These tokens are randomly generated and have no intrinsic value, making them useless to potential attackers even if intercepted [17]–[19]. Tokenization helps protect sensitive information during transactions by ensuring that the original data is never transmitted or stored in its entirety. Instead, only the token is used to represent the data, reducing the risk of data breaches and unauthorized access [20], [21].

The Secure Element (SE) is a tamper-resistant hardware component embedded in devices such as smartphones, smart cards, and payment terminals [22]. It provides a secure environment for storing sensitive information and executing cryptographic operations, such as encryption and decryption. The Secure Element is isolated from the device's main operating system and inaccessible to unauthorized applications, enhancing its security [23]–[25]. It is commonly used to store payment credentials, authentication keys, and other sensitive data, enabling secure transactions and interactions with various services, including mobile payments, digital wallets, and authentication systems.

To enhance security, digital wallets employ tokenization technology. Instead of storing actual credit card numbers, digital wallets generate unique, one-time tokens for each transaction. These tokens are then securely stored in a dedicated chip called the Secure Element, which is isolated from the device's main operating system, providing an additional layer of protection against fraudulent activities.

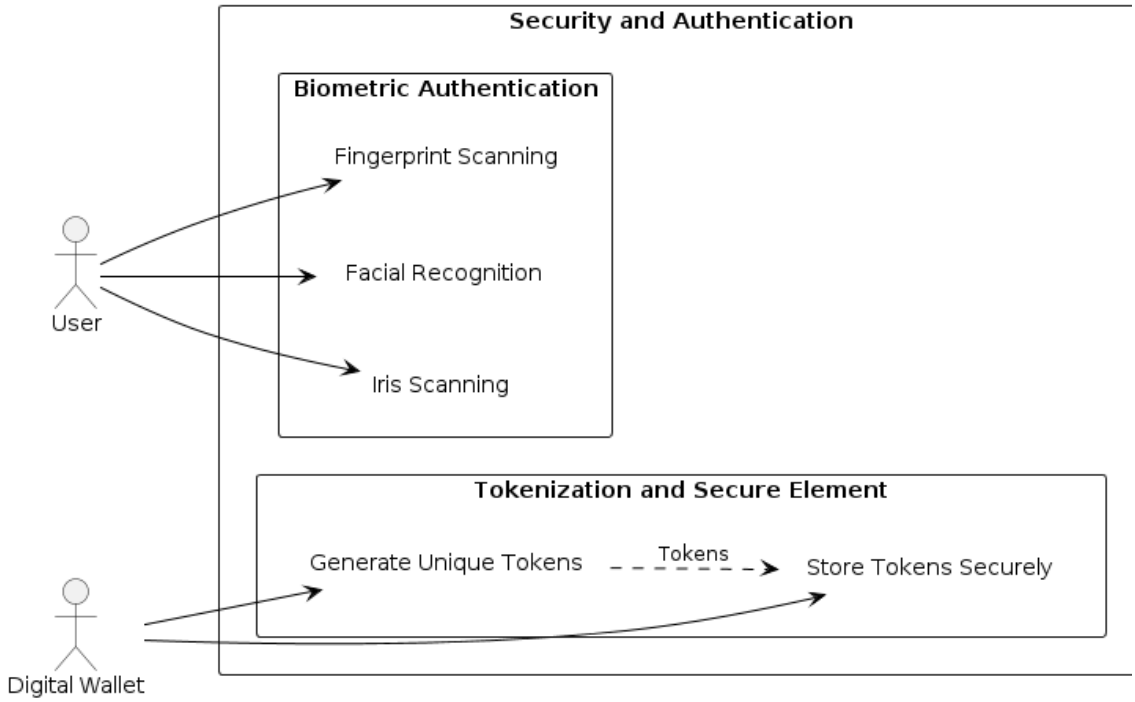
2. Biometric Authentication:

Biometric authentication is a security method that uses unique biological characteristics to verify the identity of an individual. These biological traits can include fingerprints, iris patterns, facial features, voiceprints, and even behavioral characteristics like typing patterns or gait [26], [27]. Biometric authentication systems capture and analyze these traits to confirm a person's identity for providing a secure and convenient method of access control.

The primary components of biometric authentication systems include a sensor or scanner to capture the biometric data, software to process and analyze the data, and a database to store reference templates for comparison [28], [29]. During authentication, the system compares the captured biometric data with stored templates to determine if there is a match. If the biometric data matches the stored template within an acceptable margin of error, the individual's identity is confirmed,

granting access to the secured system or facility.

Figure 3. Security and Authentication in Digital Wallets



Digital wallets have integrated biometric authentication methods to verify user identity and authorize transactions. Fingerprint scanning, facial recognition, and iris scanning have become common features in smartphones and smartwatches, adding an extra level of security to contactless payments. Biometric authentication ensures that only the authorized user can access the digital wallet and initiate transactions.

Device Integration

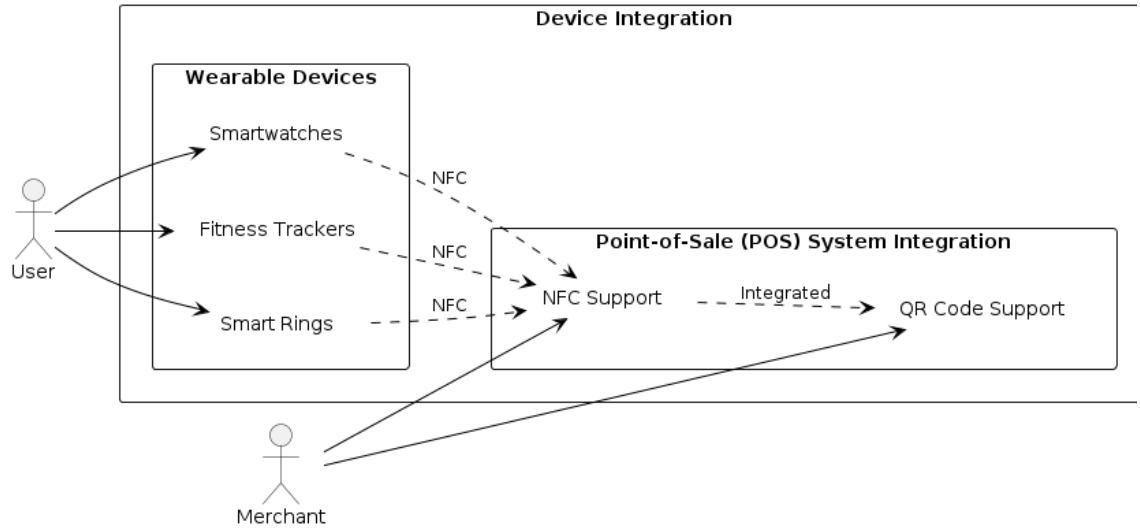
1. Wearable Devices:

Wearable devices are electronic gadgets or accessories that can be worn on the body, typically designed to perform specific functions or tasks. These devices often incorporate sensors, processors, and wireless connectivity to collect data, track activities, and provide feedback or information to the user. Wearable devices come in various forms, including smartwatches, fitness trackers, smart glasses, and health monitoring devices.

The components of wearable devices vary depending on their intended purpose and features, but common elements include sensors for monitoring biometric data such as heart rate, activity level, and sleep patterns; processors for data processing and analysis; displays for presenting information to the user; and batteries or power sources for energy supply. Many wearable devices also feature wireless connectivity, such as Bluetooth or Wi-Fi, to sync data with smartphones or other devices, enabling users to access and analyze their data remotely.

The integration of digital wallets has extended beyond smartphones to include wearable devices such as smartwatches, fitness trackers, and even smart rings. These devices are equipped with NFC technology, allowing users to make contactless payments conveniently without the need to take out their phones or wallets.

Figure 4. Device Integration in Digital Wallets



2. Point-of-Sale (POS) System Integration:

A Point-of-Sale (POS) system is a computerized system used by businesses to complete sales transactions. It typically consists of hardware and software components that work together to process payments, manage inventory [30], [31], and generate sales reports. The primary components of a POS system include a terminal or device for capturing sales information, such as a cash register, tablet, or dedicated POS terminal; software for processing transactions, managing inventory, and generating reports; and peripheral devices such as barcode scanners, receipt printers, and card readers.

POS systems streamline the checkout process by allowing businesses to ring up sales, accept payments, and issue receipts quickly and efficiently. They can process various payment methods, including cash, credit and debit cards, mobile payments, and electronic wallets, providing customers with flexibility and convenience [32], [33]. POS systems often integrate with inventory management software, allowing businesses to track stock levels in real-time, reorder products when inventory runs low, and generate reports on sales trends and performance.

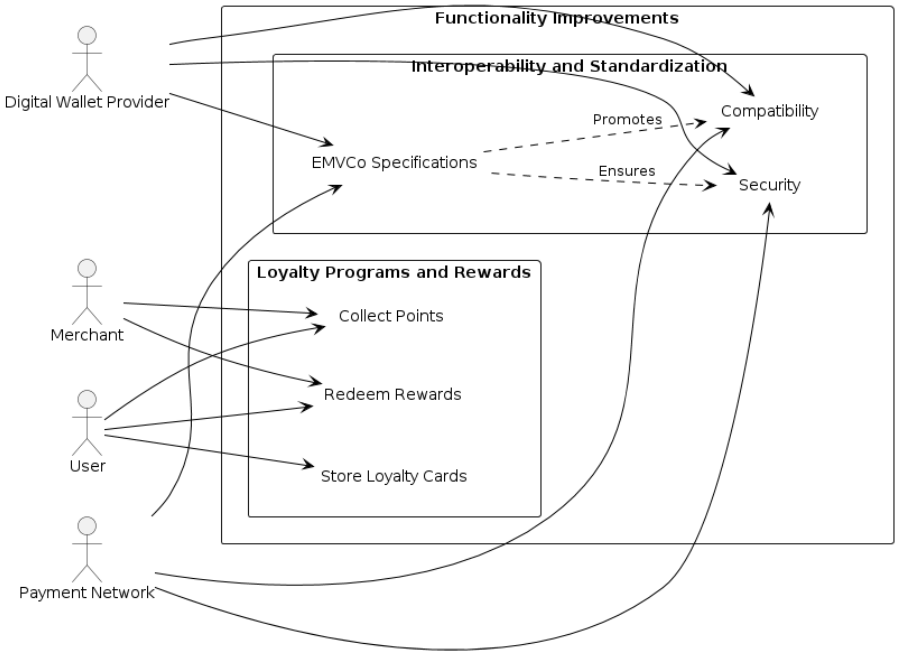
Contactless payment technologies have been seamlessly integrated into modern POS systems. Retailers and businesses have upgraded their payment terminals to support NFC and QR code transactions. This integration enables merchants to accept digital wallet payments effortlessly, improving the checkout experience for customers.

Functionality Improvements

1. Loyalty Programs and Rewards:

Loyalty programs and rewards are marketing strategies designed to incentivize customer loyalty and encourage repeat business [34], [35]s. These programs are commonly employed by businesses across various industries, including retail, hospitality, and e-commerce, to cultivate long-term relationships with customers and drive sales. The core components of loyalty programs typically include rewards, incentives, and membership tiers [36].

Figure 5. Functionality Improvements in Digital Wallets



Rewards can take many forms, such as discounts, coupons, free merchandise, exclusive access to events or promotions, or points that can be redeemed for products or services. Incentives are offered to customers as a reward for engaging with the business, making purchases, or taking specific actions, such as referring friends or completing surveys. Membership tiers often categorize customers based on their level of engagement or spending, with higher tiers offering greater rewards and benefits.

Loyalty programs and rewards are used for both businesses and customers. For businesses, loyalty programs can increase customer retention, boost sales, and generate valuable customer data and insights. Businesses can enhance the overall customer experience and improve the effectiveness of their marketing efforts by tailoring rewards and incentives to individual customers, tracking customer behavior and preferences.

Digital wallets have gone beyond mere payment functionality by integrating loyalty programs and rewards systems. Users can store their loyalty cards, collect points, and redeem rewards directly through their digital wallets. This integration provides a

more streamlined and convenient way for consumers to manage their loyalty memberships and take advantage of exclusive offers. Efforts have been made to ensure interoperability and standardization among different digital wallet providers and payment networks. Organizations have developed specifications and certifications to promote compatibility and security across various contactless payment systems. This standardization allows users to use their digital wallets across a wide range of merchants and payment terminals.

Conclusion

The integration of digital wallets and contactless payment technologies has significantly transformed the way consumers make transactions, offering a new level of convenience, security, and efficiency. Near Field Communication (NFC) technology has been at the forefront of this revolution, enabling digital wallets to facilitate secure and seamless transactions [37], [38]. Users can complete a transaction without the need for physical cash or credit cards by simply tapping their smartphone or smartwatch on an NFC-enabled payment terminal. This technology has gained widespread adoption, with major retailers and businesses upgrading their payment infrastructure to support NFC transactions.

In addition to NFC, QR code payments have emerged as another popular contactless payment method. Digital wallets like Alipay and WeChat Pay have leveraged QR codes to allow users to initiate payments by scanning codes displayed by merchants. The versatility of QR codes has led to their integration into various devices, including wearables and even tattoos, expanding the possibilities for contactless payments beyond smartphones.

To address security concerns, digital wallets have implemented advanced security measures such as tokenization and the use of Secure Elements. Instead of storing sensitive credit card information directly, digital wallets generate unique, one-time tokens for each transaction. These tokens are then securely stored in a dedicated chip called the Secure Element, which is isolated from the device's main operating system. This approach provides an additional protection against fraudulent activities, as the actual credit card numbers are never exposed during transactions.

Digital wallets have integrated biometric authentication methods to verify user identity and authorize transactions. Fingerprint scanning, facial recognition, and iris scanning have become standard features in modern smartphones and smartwatches, adding an extra level of security to contactless payments. Digital wallets reduce the risk of unauthorized access or theft by requiring biometric authentication, ensuring that only the authorized user can access the wallet and initiate transactions.

The integration of digital wallets has also extended to wearable devices, offering users even greater convenience and flexibility. Smartwatches, fitness trackers, and smart rings equipped with NFC technology allow users to make contactless payments without the need to take out their phones or wallets. This seamless integration has made it easier for consumers to make quick and secure transactions on the go, whether they are at a retail store, restaurant, or public transit system.

To support the growing adoption of contactless payments, retailers and businesses have upgraded their point-of-

sale (POS) systems to accommodate NFC and QR code transactions. This integration has streamlined the checkout process for reducing queues and improving the overall customer experience. Merchants can now accept digital wallet payments effortlessly, without the need for additional hardware or complex setup processes.

Beyond mere payment functionality, digital wallets have also incorporated loyalty programs and rewards systems, providing added value to consumers. Users can store their loyalty cards, collect points, and redeem rewards directly through their digital wallets, eliminating the need to carry physical loyalty cards. This integration has made it more convenient for consumers to manage their loyalty memberships and take advantage of exclusive offers, enhancing their overall shopping experience.

To ensure interoperability and compatibility across different digital wallet providers and payment networks, many organizations have developed specifications and certifications. These standards promote seamless integration and security across various contactless payment systems, allowing users to use their digital wallets at a wide range of merchants and payment terminals. Standardization efforts have been crucial in driving the widespread adoption of contactless payments and building consumer trust in the technology.

As with any technology that involves sensitive financial information, robust security measures and regular updates are essential to mitigate risks and protect user data. Digital wallet providers must continually invest in advanced security technologies and collaborate with financial institutions and payment networks to ensure the highest level of protection. While major retailers and businesses have embraced contactless payments, smaller merchants may face barriers in terms of costs and technical implementation. Encouraging the adoption of contactless payment technologies among small and medium-sized businesses is crucial to achieving ubiquitous acceptance and realizing the full potential of digital wallets.

User education and awareness also play a significant role in the success of digital wallets and contactless payments. Some consumers may be hesitant to adopt new payment methods due to concerns about security or a lack of familiarity with the technology. Effective communication and educational initiatives are necessary to address these concerns, highlight the benefits of contactless payments, and provide clear instructions on how to use digital wallets safely and efficiently.

The exploration of biometric-based authentication methods, such as palm vein scanning, could further enhance the security and convenience of contactless payments. These authentication methods could provide an even higher level of assurance and reduce the reliance on traditional PIN or password-based systems by leveraging unique biological characteristics.

References

[1] A. Cole and S. McFaddin, “Toward a mobile digital wallet,” *New York: IBM*, 2009.

[2] R. K. Balan and N. Ramasubbu, “The digital wallet: Opportunities and prototypes,” *IEEE Computer*, 2009.

[3] E. Benli, I. Engin, C. Giousouf, M. A. Ulak, and Ş. Bahtiyar, “BioWallet: A Biometric Digital Wallet,” *ICONS 2017*, 2017.

[4] A. J. Levitin, "Pandora's digital box: The promise and perils of digital wallets," *Univ. PA Law Rev.*, 2017.

[5] O. Alaeddin, R. Altounjy, Z. Zainudin, and F. Kamarudin, "From physical to digital: Investigating consumer behaviour of switching to mobile wallet," *Pol. J. Manag. Stud.*, Jun. 2018.

[6] D.-H. Shin, "Towards an understanding of the consumer acceptance of mobile wallet," *Comput. Human Behav.*, vol. 25, no. 6, pp. 1343–1354, Nov. 2009.

[7] M. Arora and M. P. Yadav, "A Study on Perception of Different Generation in the Use of E Wallet," *Journal of IMS Group*, 2018.

[8] M. Olsen, J. Hedman, and R. Vatrapu, "e-Wallet Properties," in *2011 10th International Conference on Mobile Business*, 2011, pp. 158–165.

[9] P. Sunny and A. George, "Determinants of behavioral intention to use mobile wallets--a conceptual model," *J. Manage.*, 2018.

[10] V. Coskun, B. Ozdenizci, and K. Ok, "A survey on near field communication (NFC) technology," *Wirel. Pers. Commun.*, vol. 71, no. 3, pp. 2259–2294, Aug. 2013.

[11] Y. Y. Yen*, G. S. Ruey, D. A. Rasiah, T. K. Sin, L. K. Piew, and S. A. Ramasamy, "User acceptance of near field communication (NFC) system," in *The European Proceedings of Social and Behavioural Sciences*, 2018.

[12] T. J. Soon, "QR code," *synthesis journal*, vol. 2008, pp. 59–78, 2008.

[13] J. Lee, C.-H. Cho, and M.-S. Jun, "Secure quick response-payment(QR-Pay) system using mobile device," in *13th International Conference on Advanced Communication Technology (ICACT2011)*, 2011, pp. 1424–1427.

[14] A. Surekha, P. M. R. Anand, and I. Indu, "E-payment transactions using encrypted QR codes," *International Journal of Applied*, 2015.

[15] J. Lu, Z. Yang, L. Li, W. Yuan, L. Li, and C.-C. Chang, "Multiple Schemes for Mobile Payment Authentication Using QR Code and Visual Cryptography," *Mobile Information Systems*, vol. 2017, Mar. 2017.

[16] S. Gao, X. Yang, H. Guo, and J. Jing, "An Empirical Study on Users' Continuous Usage Intention of QR Code Mobile Payment Services in China," *IJEA*, vol. 10, no. 1, pp. 18–33, Jan. 2018.

[17] T. Bradford, "The Puzzle of Payments Security: Fitting the Pieces Together to Protect the Retail Payments System," *Payments System Research Briefing*, 2015.

[18] Z. C. Nxumalo, P. Tarwireyi, and M. O. Adigun, "Towards privacy with tokenization as a service," in *2014 IEEE 6th International Conference on Adaptive Science & Technology (ICAST)*, 2014, pp. 1–6.

[19] M. Crowe, S. Pandy, D. Lott, and S. Mott, "Is Payment Tokenization Ready for Primetime?," *dated Jun*, vol. 11, p. 51, 2015.

[20] P. Janulek, "Tokenization as a Form of Payment and Valuation Professional, Scientific, Specialist and Technical Activities," *, Specialist and Technical Activities (December 27 …*, 27-Dec-2018.

[21] H. J. Yoo, S. Lee, S. Jang, and M. Jung, "Study of Tokenization for Easy Payment System on Mobile Platform," *Information Institute (Tokyo) …*, vol. 18, no. 12, pp. 5091–5096, Dec. 2015.

[22] G. Madlmayr, J. Langer, C. Kantner, and J. Scharinger, "NFC Devices: Security and Privacy," in *2008 Third International Conference on Availability, Reliability and Security*, 2008, pp. 642–647.

[23] M. Green and I. Miers, "Bolt: Anonymous Payment Channels for Decentralized Currencies," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, Dallas, Texas, USA, 2017, pp. 473–489.

[24] C. Morosan and A. DeFranco, "It's about time: Revisiting UTAUT2 to examine consumers' intentions to use NFC mobile payments in hotels," *Int. J. Hosp. Manage.*, vol. 53, pp. 17–29, Feb. 2016.

[25] T. Washiro, "Applications of RFID over power line for Smart Grid," in *2012 IEEE International Symposium on Power Line Communications and Its Applications*, 2012, pp. 83–87.

[26] D. Kumar, Y. Ryu, and D. Kwon, "A survey on biometric fingerprints: The cardless payment system," in *2008 International Symposium on Biometrics and Security Technologies*, 2008, pp. 1–6.

[27] R. K. Garg and N. K. Garg, "Developing secured biometric payments model using Tokenization," in *2015 International Conference on Soft Computing Techniques and Implementations (ICSCTI)*, 2015, pp. 110–112.

[28] N. Buchmann, C. Rathgeb, H. Baier, and C. Busch, "Towards Electronic Identification and Trusted Services for Biometric Authenticated Transactions in the Single Euro Payments Area," in *Privacy Technologies and Policy*, 2014, pp. 172–190.

[29] P. Mukhopadhyay, K. Muralidharan, P. Niehaus, and S. Sukhtankar, "Implementing a biometric payment system: The Andhra Pradesh experience," *UC San Diego Policy Report. La Jolla: UCSD*, 2013.

[30] S. I. Lestariningati, "Mobile point of sale design and implementation," *IOP Conf. Ser.: Mater. Sci. Eng.*, vol. 407, no. 1, p. 012094, Aug. 2018.

[31] M. Polasik, J. Górka, G. Wilczewski, J. Kunkowski, K. Przenajkowska, and N. Tetkowska, "Time Efficiency of Point-of-Sale Payment Methods: Empirical Results for Cash, Cards and Mobile Payments," in *Enterprise Information Systems*, 2013, pp. 306–320.

[32] A. Kabir and B. Han, "An improved usability evaluation model for point-of-sale systems," *Int. J. Smart Home*, vol. 10, no. 7, pp. 269–282, Jul. 2016.

[33] C. Parkan, "Measuring the effect of a new point of sale system on the performance of drugstore operations," *Comput. Oper. Res.*, vol. 30, no. 5, pp. 729–744, Apr. 2003.

[34] M. D. Uncles, G. R. Dowling, and K. Hammond, "Customer loyalty and customer loyalty programs," *Journal of Consumer Marketing*, vol. 20, no. 4, pp. 294–316, Jan. 2003.

[35] G. R. Dowling and M. Uncles, “Do customer loyalty programs really work?,” *Sloan Manage. Rev.*, 1997.

[36] Y. Yi and H. Jeon, “Effects of Loyalty Programs on Value Perception, Program Loyalty, and Brand Loyalty,” *Journal of the Academy of Marketing Science*, vol. 31, no. 3, pp. 229–240, Jul. 2003.

[37] G. Aydin and S. Burnaz, “Adoption of mobile payment systems: A study on mobile wallets,” *Journal of Business, Economics and Finance*, vol. 5, pp. 73–92, Mar. 2016.

[38] A. M. Franciska and S. Sahayaselvi, “An overview on digital payments,” *International Journal of Research*, 2017.