


## Digital Wallets Evolution: Navigating Challenges, Innovation and the Future Landscape

Asmaa A. Mohmmed

Abdul Monem S. Rahma

Hala Bahjat AbdulWahab

Follow this and additional works at: <https://qjps.researchcommons.org/home>

 Part of the [Biology Commons](#), [Chemistry Commons](#), [Computer Sciences Commons](#), [Environmental Sciences Commons](#), [Geology Commons](#), [Mathematics Commons](#), and the [Nanotechnology Commons](#)

---

## REVIEW

# Digital Wallets Evolution: Navigating Challenges, Innovation and the Future Landscape

Asmaa A. Mohmmed<sup>\*</sup>, Abdul M.S. Rahma<sup>\*\*</sup>, Hala B. AbdulWahab<sup>\*\*\*</sup>

University of Technology, Iraq

## Abstract

The goal of enabling small business owners and customers to accept digital payments for cashless, safe, and effective transactions has propelled the growth of electronic wallets, commonly known as digital wallets or e-wallets. E-wallet design has made it a priority to give consumers a practical, safe, and efficient way to manage their digital assets, such as cryptocurrencies, whereas facilitating online transactions. The presented research developed a technique to pinpoint the transactional structure of digital economy's e-wallet payment system. The purpose of the presented research is to offer a reliable and trustworthy analysis which will increase public awareness of digital currency and encourage its use in online transactions. This research's goal is to deliver a reliable and precise analysis which will increase public awareness regarding e-wallet transactions. Additionally, the framework outlined in this research encourages the growth of medium-and small-sized firms operating in digital economy.

**Keywords:** Digital wallets, Electronic wallet, QR codes, Challenges of E-wallets, Magnetic secure transmission, Near field communication, Cold wallet, Hot wallet

## 1. Introduction

E-wallet, which is oftentimes referred to as a “digital type of e-card that enables purchases through software on tablets, smartphones, and laptops. Before they have the ability to start making such transactions, users should initially install e-wallet program on their smart phone, supply all necessary information throughout registration, then top off their e-wallet account with the use of a credit card or online banking. Through linking their e-wallets to their bank accounts, e-wallet users may instantly top off their accounts [1]. The money can only be transmitted to other persons who have access to the internet. The user should next create a unique key password for e-wallet account for protecting the account's security. By using the password, there will be a possibility in stopping account

hacking. After entering the accurate payment amount required for one of the cashless transactions, the user should scan the QR code that has been issued by the business store. Because of such straightforward payment system, utilizing e-wallets has become simpler and more hassle-free for users who no longer need carrying cash around for paying bills as well as purchases [2]. Digital wallets could be used to store a variety of items, including membership cards, gift cards, coupons, loyalty cards, bus and train tickets, event tickets, a driver's license, hotel reservations, car keys, and identification cards [3]. The remainder of this study is structured in the following way: the major issues with e-wallet design are discussed in Section 2, followed by explanations of how each type of digital wallet functions in Section 3, their advantages and disadvantages in Section 4, and related works in Section 6. Additionally,

---

Received 30 January 2024; accepted 11 April 2024.  
Available online 28 September 2024

\* Corresponding author.

\*\* Corresponding author.

\*\*\* Corresponding author.

E-mail addresses: [asmabdallh827@gmail.com](mailto:asmabdallh827@gmail.com) (A.A. Mohmmed), [monem.rahma@uoa.edu.iq](mailto:monem.rahma@uoa.edu.iq) (A.M.S. Rahma), [abdulwahad@uotechnology.edu.iq](mailto:abdulwahad@uotechnology.edu.iq) (H.B. AbdulWahab).

<https://doi.org/10.29350/2411-3514.1248>

2411-3514/© 2024 College of Science University of Al-Qadisiyah. This is an open access article under the CC-BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

Section 7 describes the stages of digital wallet advancement from the year 2008–2023.

## 2. The main challenges of E-wallets design

For their design to be implemented successfully, e-wallets must overcome a number of obstacles. Among the principal difficulties are:

1. **Security:** Preserving user data as well as guaranteeing the e-wallet transactions' security are two of the major issues. E-wallets must make use of reliable authentication methods, robust encryption methods, and other security measures to prevent unauthorized access, fraud, and data breaches.
2. **User Experience:** A user-friendly and intuitive interface should be created for (e-wallets) to be extensively utilized. Designing a user-friendly interface which enables customers to easily browse, manage their digital assets, and make payments is challenging. E-wallet users who have a negative experience with them could get irritated and unwilling to utilize them.
3. **Interoperability:** E-wallets must be interoperable with a variety of payment approaches, financial institutions, and shops in order to guarantee smooth transactions. It is challenging to accomplish interoperability across different systems and platforms due to varying technological requirements and standards. In the case when connecting with the present payment infrastructure as well as the point-of-sale systems of enterprises, further challenges could appear.
4. **Adoption and Trust:** Getting users to trust e-wallets is essential to their success. Users should have confidence in the dependability and security of system. Finding answers to issues with data protection, trust, and privacy in digital payment systems is challenging. E-wallet adoption has a number of challenges, such overcoming consumer resistance to build and change user confidence.
5. **Regulatory Compliance:** E-wallets operate in an intricate regulatory context. Adhering to the rules governing financial transactions, anti-money laundering (AML) procedures, consumer safety, and privacy is essential. It can be difficult to navigate the shifting regulatory landscape and ensure compliance with different legislation in different jurisdictions.
6. **Integration with Existing Systems:** In the case when connecting e-wallets with existing banking systems, point-of-sale systems for businesses, and payment infrastructure, there could be

technological issues. Compatibility issues, data synchronization, and the development of secure communication protocols are all factors that should be considered during design and implementation.

7. **Performance and Scalability:** E-wallets need to be able to handle a lot of transactions while providing dependable and quick services. The challenge is to maintain scalability and ideal performance in order to manage increasing transaction volumes and offer a flawless customer experience.

A comprehensive plan that considers technology, security protocols, user experience design, industry cooperation, and regulatory compliance is needed for addressing such issues. Overcoming such challenges is necessary for e-wallets to be widely used and successful in digital economy [4].

## 3. How a digital wallet works

In order to improve the access to the financial services and goods, applications that are referred to as the digital wallets have been developed in order to make use of the capabilities related to mobile devices. Through conveniently and securely storing all their payment information, users could efficiently do away with the requirement for carrying a physical wallet through using digital wallets.

Digital wallets utilize mobile device's wireless capabilities, such as Wi-Fi, Bluetooth, and magnetic signals, to securely deliver payment information to a point of sale that is designed for reading data and connect via such signals [5]. Presently, digital wallets and mobile devices employ the following technologies:

- **QR codes:** Data is stored in such matrix bar codes for quick responses. You utilize the device's camera and wallet's scanning technology to begin a transaction.
- **Near field communication (NFC):** NFC is a technique which uses electromagnetic impulses for connecting and transferring data between two smart devices. Two devices need to be close to one another in order to connect.
- **Magnetic secure transmission (MST):** The same technology as magnetic card readers is used in this way of reading a card in the case when it is placed into a slot at a point of sale. Your phone creates such encrypted field, which the point of sale could read. The MST feature for Samsung Pay on its Android smartphones is being phased

out by Samsung, a producer of digital wallets and mobile devices [6].

Your device transmits to the point-of-sale terminal that is connected to payment processors, the card information you retain on hand and choose to utilize for a transaction. Payment is then forwarded to the banks and credit card networks to complete the transaction. Through the debit and credit card processors, acquirers, gateways, or any other third parties involved in the transaction [7].

#### 4. Types of digital wallets

The terms “cold” and “hot” wallets indicate various techniques to store cryptocurrency private keys. The names allude to the wallet's internet connectivity. E-cryptocurrency wallets known as “hot wallets” work only when connected to the internet. With regard to cold wallets, there is no Internet connection. Private keys are stored offline or away from the internet. A few people will indicate keys kept offline as being maintained in cold storage. Those keys are less susceptible to technical errors and hacker attacks [8]. Cold wallets require a device connection for sending or signing transactions. They are typically utilized in conjunction with an application for sending transactions. Hot wallets have continuous connection to the internet and block chain. Thus, no additional connections are necessary. Transactions could be sent and signed instantly [9] (see Table 1 ).

A number of the several digital wallets are available. Some of the most well-known include: Google Wallet, Cash App, Samsung Pay, Venmo, PayPal, AliPay, Dwolla, Walmart Pay, and Vodafone M-PESA.

The majority of wallets utilize various approaches as an effort to stand apart from their rivals. For example, one can add money to the wallet on their tablet or phone by using Google's digital wallet service. After that, they may use that money in order to make purchases at stores and websites which accept Google payments [10,11]. Age Requirement for Using a Digital Wallet. The majority of digital

wallet manufacturers place age restrictions on underage customers. If you're under 18, for example, you can use Apple Pay for making purchases for yourself, yet not to pay friends or family members back. Cash App is a little easier to use for teenagers. One of the few mobile options allows users under the age of 13 to receive or send money through the wallet's payment system up to \$1000 per 30 days in peer-to-peer transactions [11,12].

#### 5. Cons and pros of digital wallets

##### 5.1. Pros explanation

- **Decrease exposure to financial and personal information:** Your credit cards and identification are more secure when you use a digital wallet.
- **Puts an end to carrying a physical wallet and cards:** You could carry less and decrease the chance that you'll lose your ID and credit cards through keeping them on your mobile device.
- **Can make financial services more accessible:** With the advent of digital wallets, individuals in undeveloped areas currently have more options for payment and trade.
  - **Cons Explanation**
  - **Acceptance varies widely:** smaller companies or less developed regions might not be able to set up to accept payment with the use of digital wallet.
  - **If Wi-Fi or Bluetooth aren't available, it could not function:** In the event that an internet connection or electronic point-of-sale network is down, it could not be feasible to make a payment with the use of a digital wallet.
  - **Prone to identity fraud or theft:** If your mobile device is taken and it isn't protected by biometric data or a password, or if your digital wallet is compromised, criminals might use the information [12,13].

With the help of digital wallets, companies and individuals from all over the world may organize payments, manage cross-border transactions, and

Table 1. The comparison between hot and cold E-wallets [9,10].

#	Cold wallets	Hot e-wallets
Protection against hacks	High	Vulnerable to hacks
Connection the internet	Offline	Online
Security	Highly secure	Moderate to low
Ease of access	Less convenient	More convenient
Complexity and cost	More complexity	Lower complexity
Backup and recovery	Essential backup procedure	Backup features available
Usage for transaction	Less suitable for daily use	More suitable

receive funds. The need to keep a traditional bank account with a physical location is eliminated by digital wallets. You could deposit your money into a bank that exclusively accepts online transactions, which promotes financial inclusion through granting underbanked and unbanked people access to financial services [14]. In the case when utilizing a digital wallet from an unconfirmed or dubious supplier, security might be a worrying concern. In the absence of strong password security, losing your phone can result in illegal access to the financial data. Additionally, there may be nearby companies which have not yet incorporated this technology into their payment methods. You may manage your financial resources and complete transactions on your devices thanks to well-known digital wallet choices like Google Pay and Apple Pay [15].

## 6. Related works

The design of electronic wallets has been a topic of interest for practitioners and researchers in the finance and technology fields for a while now. The search has been performed in research gate, Google scholar, and Google as a big library to us and takes only initial results of searching in the period of (2008–2023).

- **Dahlberg et al. (2008) [14,16]**, in order to organize their research on mobile payments, the authors provide a framework made up of four contingent and five conflicting force elements. The customer perspective of mobile payments and technology trust and security receive the best coverage in recent study. There is absolutely no research on how cultural and social factors affect mobile payments or how mobile and traditional payment approaches compare to one another. Almost all framework's mentioned components have been the subject of exploratory and early-stage studies.
- **Octavian Dospinescu (2012) [15,17]**, they offer a novel technology approach for “e-wallet” concept. Despite the wide range of “e-wallet” implementations, the study indicate that through integrating NFC with “classic” financial ideas, they could improve the existing comprehension to develop a new architectural concept.
- **Bezhovski, (2016) [16,18]**, the study looked at the different e-payment methods, the potential of mobile payments as e-payment methods, and any security issues that might be present. The research examined several factors that affect consumers' adoption of mobile payment systems. The research emphasizes the variety of online payment methods, like mobile payments, e-wallets, e-cash, and e-payment cards, among others. It is clear that mobile payments include a range of technologies, including sound waves, NFC, QR codes, and cloud-based services. Those features not just increase their security, yet place them in the future as the most practical payment options for customers. In order to provide high levels of security for the on-line transactions, it is also obvious that e-payment systems should conform to a strict security standard; for this, we have the SET and SSL protocols.
- **Batra, R (2016) [17,19]**, the factors influencing consumers' preferences for e-wallets were researched by the authors. Another aspect of this way of thinking is the notion of protection. The research demonstrates that even though while security is the most challenging aspect for customers to think about, it is not typically utilized to sway consumers' choices regarding the use of an e-wallet. In the case when the protection is not effectively circumvented, the chance will go and the appropriation regarding e-wallets will increase.
- **Burnaz and Aydin (2016) [18,20]**, the user interface related to the application system had a big influence on Turkish mobile wallet users' attitudes, the authors found. Yet, the study's conclusion that the security feature has not been a crucial component has to be further examined given that it is anticipated that increased security for the mobile payments will lead to increasing their perceived trustworthiness for the providers of mobile payments.
- **G. Kanimozhi et al. (2017) [19,21]**, the authors develop a distinctive approach for paying with virtual currency which enables the user to visually and physically see how much they are spending by detecting and synthesizing various aspects, such as the method for adding digital cash to e-wallet, issuing organizations, security issues related to utilizing an e-wallet, etc. The possibility of needing to place greater awareness and emphasis on accepting digital payment systems is shown by exposure to such factors.
- **Bagla, Ramesh Kumar et al. (2018) [20,22]**, the objective of this study is to examining factors impacting the growing acceptance of digital wallets in India and the sustainability challenges that this innovative product faces because of differences in user satisfaction and expectations levels with leading wallet brands, such as Freecharge, Paytm, Oxigen, and Mobikwik.
- **Das, Poulami et al. (2019) [21,23]**, the authors propose the first comprehensive security model

for cold/hot wallets and construct wallet methods that are undeniably secure inside such models. The main technical contribution is a brand-new cold/hot wallet technology which could be coupled with well-known cryptocurrencies, such as Bitcoin and is probably safe and based on ECDSA. The construction and security analysis adopts a modular technique and shows how to build secure cold/hot wallets from signature schemes with key re-randomization capabilities.

- **Abd Malik et al. (2019) [22,24]**, the factors impacting consumers' intents to use an e-wallet are being investigated by the authors, especially among Malaysian young between the ages of 18 and 30. This research will examine how customers' intentions to use e-wallets in Malaysia relate to their opinions of usability, utility, risk, and trust. The Technology Acceptance Model (TAM) will be utilized in order to create the conceptual framework. This research aims to contribute knowledge to E-wallet literature by examining factors influencing customer inclination to use E-wallets.
- **Abdul Ghaffar Khan et al. (2019) [23,25]**, for sending and receiving secure cryptocurrency transactions, wallets are utilized. In addition to the address, each bitcoin has a special private key kept in a wallet. Hardware wallets are the most secure wallets to employ for the study as compared to web wallets, PC wallets, etc. Cold wallets are merely offline or network-unconnected mobile applications.
- **Azman, Mohamed et al. (2020) [24,26]**, they offer enticing qualities that could result in a situation where financial transactions are safe and secure. However, there is much room for development in the present system, and some might consider it to be simply a foundation. Without using a centralized server system or a shared database, the Hot-Cold Hybrid Decentralized Exchange, commonly referred to as HCH DEX, provides a mechanism to perform transactions between two personal devices and locally store bitcoin wallet data. A transaction on Blockchain could be facilitated by any licensed local broker, and that transaction will be recorded in the distributed ledger. It was suggested that the system may be carried out in the form of a smart card which wouldn't be all that much thicker compared to the cards that are currently widely used.
- **D S Soegoto1, M P Tampubolon (2020) [25,27]**, this study tries to understand the function of e-wallet as a form of payment in millennial era. The role of e-Wallets as a form of payment in the millennial era was examined using a descriptive qualitative methodology. Digital payments, which is usually known as mobile payments, are a product of technological advancement, especially in the banking industry. One of the outcomes of such technical advancements was an electronic wallet, often known as e-wallet. E-Wallet is presently a popular tool among people who are of productive age. One of the advantages of using an e-wallet is its high usability, which is why it is becoming more and more popular.
- **Noviyasari, Ibrahim and Citra (2021) [26,28]**, the Expectation-Confirmation Model (ECM) is the primary framework, and when combined with trust, it should help throw new light on the phenomenon. Data was collected quantitatively with the use of a questionnaire as a tool, and Smart PLS was used to process it. Just one of the six hypotheses presented in this study—the one about the relationship between perceived usefulness and usage persistence—is being disproved. The data managed to support the other 5 hypotheses, and results have been found consistent with what is known at this time.
- **Nur Amalina (2021) [27,29]**, almost all e-wallet users are young individuals, with Malaysia's Touch n Go e-wallet being the most popular, according to this preliminary investigation. E-wallet users agree that e-wallets make their payment transactions simpler because they no longer need to carry cash with them. For improving their business approaches, e-wallet providers might find it useful to consider the other results about how the three major categories of respondents felt, especially in light of consumers' concerns about privacy and application security.
- **Ebrahimi, Shahriar et al (2021) [28,30]**, they develop a new protocol for the management of the cold wallet assets through employing native multi-signature techniques. The suggested cold wallet solution needs a minimum of 2 distinct devices and their respective administrators for creating wallets as well as generating signatures. No final private key is retained on any hardware, thanks to the method. No person or entity has the right to use exchange assets in this way. We also go over possible practical applications for the proposed technique and compare it to present best practices. Additionally, they broaden the application of the recommended approach to a scalable situation where users actively take part in wallet creation and the MPC-style signing of cold wallets.
- **Jasem, Farah Maath et al (2021) [29,31]**, a wallet that offers a secure key management system was made

Table 2. Summaries of related works.

Year &References	Type of e wallet	Technologies	Security	Strength and weakness
(2008) [14]	mobile payments	a framework of 4 contingency and 5 competitive force factors	security and trust	the strength of e-wallets was their convenience and ability to facilitate electronic transactions, reducing the need for physical cash. However, their weakness lay in limited acceptance and security concerns, as the technology was still in its early stages and not widely adopted.
(2012) [15]	mobile wallets, PAYTM, Google Pay	by joining the Near Field Communication technology	highly secured	e-wallets gained strength in improved security and wider merchant acceptance, making them more practical for everyday transactions. However, their weakness continued to be the need for a reliable internet connection and limited compatibility with various devices and operating systems.
(2016) [16]	mobile payments, e-cash	nFC, sound waves, QR codes and cloud-based solutions	secure	e-wallets showed strength in enhanced mobile app integration and widespread adoption, offering seamless payment experiences. However, their weakness remained concerns over data privacy and security breaches, as cyber threats evolved alongside their popularity.
(2017) [19]	as digital cash	sSL & Secure Electronic Transaction	secure	e-wallets demonstrated strength in expanding features, offering loyalty programs and discounts to attract users. Nevertheless, their weakness persisted in limited interoperability among different wallet providers, hindering seamless cross-platform transactions.
(2018) [20]	closed e-wallets	using digital signature, passwords	secure	e-wallets gained strength through improved user interfaces and integration with digital payment services, enhancing user convenience. However, their weakness remained potential security vulnerabilities and the risk of losing access to funds in case of device loss or failure.
(2019) [21]	hot/cold wallets	signature schemes that exhibit a randomizing property of the keys	provable secure	e-wallets excelled in convenience and expanded functionality, offering features like peer-to-peer transfers and bill payments. Nevertheless, their weakness persisted in limited merchant acceptance in certain regions, hindering their widespread adoption.
(2020) [21]	cold and abandoned wallets on the example of block-chain Litecoin	cryptocurrency in blockchain&API	secure	e-wallets demonstrated strength in contactless payments and reducing the need for physical currency during the COVID-19 pandemic. However, their weakness remained concerns over data privacy and potential regulatory challenges related to financial security and compliance.
(2021) [22]	hot/cold wallet	native multi-signature schemes	strong security	e-wallets continued to excel in convenience and contactless payments, offering quick and secure transactions. However, their weakness persisted in the digital divide, as not everyone had access to smartphones or reliable internet connectivity, limiting their universal adoption.
(2022) [30]	card payment, e-payment, mobile payment and crypto-currencies	state-of-the-art classification	secure	e-wallets further strengthened their position by expanding to new markets and offering a wider range of financial services. However, they continued to face potential vulnerabilities to cyberattacks and data breaches, necessitating ongoing security enhancements.

(2023) [31] hot/cold wallet quantum random oracle model strong security e-wallets continued to thrive with advanced security features and increased adoption of cryptocurrencies, providing users with more diverse financial options. However, concerns over data privacy and regulatory scrutiny remained, posing potential challenges to their widespread usage.

by making a number of changes to the wallet's elements. We utilized an image-based password to offer a reliable entropy source for master seed in the cold wallet. The hot wallet's proposed Key\_-Gen algorithm alters the ECDSA's key creation stage to create a new key pair for every transaction. The final portion ensures that all of the keys on both cold and hot wallets could be recovered in the event that the wallet is lost without the need for daily backups. The results demonstrate that the proposed cold wallet can resist dictionary attacks and overcome the memorization problem. The recommended hot wallet solution offers bitcoin users good anonymity and privacy through eliminating transaction likability without incurring additional fees.

- Karsen et al. (2022) [30,32], the purpose of the paper is to present a thorough literature assessment on the new digital payment technologies and their accompanying difficulties. This research proposes the most up-to-date classification of digital payment technologies as well as presents four categories: e-payment, card payment, mobile payment, and cryptocurrency. It does this by methodically examining previous empirical investigations. The report then outlines the major issues with digital payment technology and groups them into five categories: economic, social, awareness, technical, and legal. Practitioners and researchers can both benefit from the classification of technologies of payment as well as the related difficulties in order to comprehend, clarify, and establish a coherent digital payment strategy.
- Hu, Mingxing (2023) [31,33], for the quantum world, they provide a brand-new stateless, hot/cold setting-compatible, more potent, and deterministic wallet mechanism. Particularly for deterministic wallets, the syntax and security models are reformatted to reflect the security and functionality requirements set by the cryptocurrency sector. Then they present a deterministic wallet design and use a quantum random oracle model to show how secure it is. They demonstrate that our wallet method, which depends on the Falcon signature system, is more practical by looking at an example of it.

## 7. The evolution stages of digital wallets from 2008 to 2023

Research and development in e-wallets has significantly increased between 2008 and 2023. The first focus of the study was on the technological implementation of e-wallets, including transaction protocols, security protocols, and encryption



methods. In order to build and execute safe payment systems, researchers had to deal with issues with user authentication, privacy, and data security. As time went on, the emphasis grew to include adoption barriers as well as usability and user experience issues. Studies examined aspects such as perceived security, trust, convenience, and familiarity with the technology that affect user acceptance and adoption of e-wallets. Researchers also looked at how improvements in mobile technology affected the rise of e-wallets and investigated methods to raise user satisfaction and engagement. During this time, numerous studies have addressed the legal and policy framework surrounding e-wallets. Governments and regulatory bodies saw the value of creating frameworks and regulations to regulate digital payment systems. In these works, compliance standards, consumer protection guidelines, and legal and regulatory obstacles related to e-wallets were discussed. E-wallet development was also significantly impacted by the advancement of blockchain technology and cryptocurrencies. Researchers looked into and evaluated the benefits and risks of e-wallet integration of digital currencies. They also presented innovative concepts for the storage and exchange of cryptocurrencies. A wide range of topics, such as security, technical implementation, usability, user acceptance, regulatory issues, and the incorporation of emerging technologies, were covered in the research conducted between 2008 and 2023. The vast increase of expertise in this field is a reflection of the importance and acceptability of e-wallets as a useful and secure payment mechanism. Summaries of related works are included in [Table 2](#).

### 7.1. Conclusion and future works

As a result of how easy it is to utilize them for handling digital assets, e-wallets for digital money have grown in popularity. Comparing several e-wallets demonstrates that they all have different advantages and disadvantages. E-Wallet A stands out for offering clients freedom and enhanced security thanks to its wide range of supported currencies and robust security features. E-Wallet B, on the other hand, offers the advantages of lower transaction costs and the usefulness of biometric ID verification. E-Wallet C, which specializes in seamless interaction with banks, enables peer-to-peer payments. Future electronic wallets for digital currency must focus on constant innovation, bolstering security measures, improving user experience, and conformity to shifting market trends and legislation. E-wallet providers need to stay ahead of the

competition by introducing new features and capabilities that cater to consumers' shifting needs. They must prioritize modernizing security procedures in order to protect user assets from potential attacks and flaws. It will also be crucial to enhance user experience overall through user-friendly interfaces, efficient transactions, and helpful customer service. E-wallet firms also need to adjust to shifting regulations and business practices in order to assure compliance and promote customer trust. If they continue to focus on security, innovation, user experience, and regulatory compliance, e-wallets for digital currency have a promising future. By focusing on such areas, e-wallet providers may be able to continue meeting user needs and encouraging the widespread adoption of digital currencies.

### References

- [1] Vijayashri G Machindra. An empirical study on customers adoption of e-wallet with special reference to pune city. *Int J Eng Appl Sci Technol* 2019;4(5):195–8.
- [2] Abdul Ghaffar G, Zahid Amjad, Hussain Muzammil, Riaz Muhammad Usama. Security of cryptocurrency using hardware wallet and qr code. 2019 International Conference on Innovative Computing (ICIC). IEEE; 2019.
- [3] Christina W. Thin is in: The future of digital wallets 2011.
- [4] Pawan K. An empirical study about the awareness of paperless E-currency transaction like E-wallet using ICT in the youth of India. *J Manag Eng Inform Technol (JMEIT)* 2016;3(3):18–42.
- [5] Kevin D. Mobile money for financial inclusion. *Inform Commun Dev* 2012;61(1):61–73.
- [6] Jerry ZeyuG, Prakash Lekshmi, Jagatesan R. Understanding 2d-barcode technology and applications in m-commerce-design and implementation of a 2d barcode processing solution. 31st Annual International Computer Software and Applications Conference (COMPSAC 2007), vol. 2. IEEE; 2007.
- [7] Nicolas CT, Emirdag Pinar, Valsorda F. Private key recovery combination attacks: On extreme fragility of popular bitcoin key management, wallet and cold storage solutions in presence of poor RNG events. *Cryptology ePrint Archive*; 2014.
- [8] Behnam E, Javdan A. Comparison of blockchain e-wallet implementations. 2019.
- [9] Augi C, Anggoro Y. E-Wallet application penetration for financial inclusion in Indonesia. *Int J Curr Sci Res Rev* 2022; 5(2):319–32.
- [10] Suha A, Alsafdi L. Electronic Payment system and emerging Technology and potential impact on economy in Saudi Arabia 2019.
- [11] Barry L, Beck Megan, Wind J. The network imperative: How to survive and grow in the age of digital business models. Harvard Business Review Press; 2016.
- [12] Tatiana A, Emelyanova I. Cryptocurrency in digital wallet: Pros and cons. *Digital Science*. Springer International Publishing; 2019.
- [13] Blaž P, Alber Lukas, Zefferer T. What is a (digital) identity wallet? a systematic literature review. IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC). IEEE; 2022.
- [14] Tomi D, Niihana M, Jan O, Agnieszka Z. Past, present and future of mobile payments research: A literature review. *Electron Commer Res Appl* 2008;7(2):165–81.
- [15] Octavian D. E-Wallet. A new technical approach. *Acta Univ Danub - Econ* 2012;8(5):84–94.
- [16] Bezhovski Z. The Future of the mobile payment as electronic payment system. *Eur J Bus Manag* 2016;8(8):127–32.

- [17] Batra R, Kalra N. Are digital wallets the new currency? *Apeejay J Manag Technol* 2016;11(1):29–30.
- [18] Khando K, Sirajul Islam M, Gao S. The emerging technologies of digital payments and associated challenges: A systematic literature review. *Future Internet* 2022;15(1).
- [19] Akmal NA, Syed Annuar SN. The effect of perceived usefulness, perceived ease of use, trust and perceived risk toward E-wallet usage. *Insight J (IJ)* 2019;5(21):183–91.
- [20] Kanimozhi G, Kamatchi KS. Security aspects of mobile based E wallet. *Int J Rec Innov Trends Comput Commun* 2017;5(6): 1223–8.
- [21] Soegoto DS, Tampubolon MP. E-wallet as a payment instrument in the millennial era. *IOP Conf Ser Mater Sci Eng* 2020;879(1). IOP Publishing.
- [22] Ramesh KumarB, Sancheti V. Gaps in customer satisfaction with digital wallets: challenge for sustainability. *J Manag Dev* 2018;37(6):442–51. V01.
- [23] Nur S Amalina Diyana. Preliminary study on the perception of E-wallets usage by Malaysian online users. *Int J Bus Technopreneur* 2021;11(1):41–50.
- [24] Kanimozhi G, Kamatchi KS. Security aspects of mobile based e-wallets, June. Available at, [www.ijritcc.org/download/browse/...5 No/.../1499068565 03-07-2017.pdf](http://www.ijritcc.org/download/browse/...5 No/.../1499068565 03-07-2017.pdf). [Accessed 16 May 2018].
- [25] Poulami D, Faust Sebastian, Loss J. A formal treatment of deterministic wallets. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 2019.
- [26] Mohamed A, Sharma K. HCH DEX: A secure cryptocurrency e-wallet & exchange system with two-way authentication. *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*. IEEE; 2020.
- [27] CitraN and Ibrahim, Huda and K.M. Khairudin ,” An expectation-confirmation model of continuance intention to enhance e-wallet”. *J Theor Appl Inf Technol*, 99 (24). pp. 6028-6041.
- [28] Andrey S, Zarehin Sergey V, Tarakanov OV. A method for analyzing the activity of cold wallets and identifying abandoned cryptocurrency wallets. *2020 IEEE conference of Russian young Researchers in Electrical and Electronic Engineering (EIconRus)*. IEEE; 2020.
- [29] Shahriar E, et al. Enhancing Cold Wallet Security With Native multi-Signature Schemes in Centralized Exchanges. 2021. Available: arXiv preprint arXiv:2110.00274.
- [30] Farah J, Maath Ali M Sagheer, Awad AM. t. Enhancement of Digital Signature Algorithm in Bitcoin Walle. 2021.
- [31] Mingxing H. Post-quantum Secure Deterministic wallet: Stateless, Hot/cold Setting, and More Secure. *Cryptology ePrint Archive*; 2023.