International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Review on Security and Privacy Considerations in Programmable Payments

Hari Prasad Josyula[1*], Latha Thamma Reddi[2], Sachin Parate[3], Arun Rajagopal[4]

Submitted: 16/10/2023 **Revised**: 06/12/2023 **Accepted**: 16/12/2023

Abstract: The paper underscores the critical importance of adopting a comprehensive approach to confront the various challenges associated with programmable payments, particularly in the context of blockchain technology and cryptocurrencies. Smart contract vulnerabilities, including coding errors and logic flaws, pose a significant risk to the integrity of financial transactions, emphasizing the need for regular security audits and testing. Additionally, the omnipresent threat of cybersecurity breaches, such as hacking and phishing, highlights the necessity of a robust security infrastructure. Balancing transparency and privacy in blockchain-based payments is a complex endeavor that requires the integration of privacy-enhancing technologies. Furthermore, navigating the evolving regulatory landscape is essential to maintain the legitimacy and trustworthiness of these systems. In essence, a multi-faceted strategy encompassing security audits, cybersecurity measures, privacy enhancements, and regulatory compliance is crucial to ensure the continued evolution of programmable payments while upholding user trust and data privacy in the financial ecosystem.

Keywords: *Digital, financial, fraud, privacy, risk, transactions*

1. Introduction

In a digital age where convenience and efficiency are paramount, programmable payments have emerged as a game-changer in the realm of financial transactions. Offering unprecedented control and customization, these payment systems are reshaping the way we interact with money. However, with great power comes great responsibility, and it is essential to examine the impact of programmable payments on security and privacy [1-2]. This comprehensive review delves into the intricate world of programmable payments, investigating the potential risks and rewards that come with this evolving technology [3]. In today's digital financial landscape, safeguarding user data is of paramount importance, given the increasing reliance on programmable payments. These payment platforms, handling sensitive financial information, are prime targets for cyber threats, necessitating robust security measures. Researchers are actively exploring cutting-edge technologies such as multi-party computation and zero-knowledge proofs to bolster privacy and security, allowing the sharing and verification of critical transaction data without compromising confidentiality [4]. Furthermore, the emergence of decentralized identity solutions empowers users by reducing dependence on centralized entities for identity verification, putting individuals in greater control of their personal data [5]. Alongside these security efforts, programmable payments cater to consumers' diverse preferences, offering a versatile range of funding sources, from bank accounts to cryptocurrencies, ensuring a universal and flexible payment experience. This continuous evolution underscores the commitment to meeting the dynamic needs and expectations of users in an increasingly digital financial world [6-7]. As hackers become increasingly sophisticated, protecting sensitive financial data is more critical than ever. We explore the security measures implemented by programmable payment platforms and assess their effectiveness in safeguarding against fraudulent activities [8]. Additionally, we examine the privacy implications of programmable payments. With transactions becoming more traceable and information being shared with various stakeholders, concerns regarding data protection and individual privacy rights arise. Is there a trade-off between convenience and privacy. The rapid evolution of programmable payments has ushered in a transformative era in the world of finance, offering a plethora of advantages that cater to both businesses and individuals. By automating financial transactions and allowing for tailored payment processes, programmable payments enhance efficiency, reduce errors, and provide a superior user experience. Moreover, their seamless integration into diverse industries and systems boosts their appeal, making

[1*]*Hari Prasad Josyula, MBA, CSPO, Senior Product Manager – Fin Tech, Princeton, New Jersey,*
Email: jhprasad@outlook.com
[2] *Latha Thamma Reddi PMP, SCM, SAP APM, FRSA, SMIEEE, Independent researcher, Program manager (Automation and Innovation), Dallas Texas*
[3] *Sachin Parate, Principal Product Manager, Independent researcher, Jersey City, New Jersey*
[4] *Arun Rajagopal, Sr. Director, AI/ML, Independent Researcher, Nutley, NJ*
***Corresponding Author:** Hari Prasad Josyula*
Email: jhprasad@outlook.com

financial management more convenient for all [9]. Nevertheless, alongside these benefits come critical challenges that demand attention. The heightened risk of security breaches and fraud necessitates rigorous security measures. Privacy concerns require robust safeguards to protect individuals' sensitive financial data [10]. Furthermore, regulatory compliance and interoperability issues must be addressed as programmable payments continue to evolve. Programmable payments and blockchain technology hold immense promise but are not without their security and privacy challenges [11]. The vulnerabilities in smart contracts, stemming from coding errors and flawed logic, pose significant risks, as they can be exploited by malicious actors, and the immutability of deployed contracts makes rectification difficult. Furthermore, the decentralized and pseudonymous nature of blockchain has attracted fraudsters engaging in scams, money laundering, and identity theft [12]. To tackle these issues, a comprehensive approach is required. This includes educating users about the inherent risks, conducting rigorous security audits, implementing regulatory frameworks, exploring technological advancements, and fostering community collaboration. The proactive efforts of researchers, developers, regulators, and the blockchain community are essential in ensuring the continued growth and security of programmable payment systems [13-15]. The provided excerpt underscores the transformative potential of programmable payments within the financial industry, emphasizing their role in differentiating and adding value to the services offered by financial institutions and fintech companies. By enabling personalized payment experiences and advanced features such as delegated authorization and just-in-time funding, these systems can cater to individual customer needs while optimizing the use of financial resources. However, it also highlights the critical importance of security and privacy considerations in this evolving landscape, as programmable payments introduce new risks related to data security, fraud, and user privacy [16]. To address these challenges, the forthcoming paper aims to provide a comprehensive analysis of the current security and privacy landscape in programmable payment systems, explore best practices and emerging technologies for risk mitigation, and ultimately offer practical recommendations for stakeholders while charting the future research and development directions in this dynamic field [17-19]. The surge in demand for these solutions has spurred research and exploration of solutions, emphasizing the need to strike a balance between innovation and maintaining essential security and privacy standards. We delve into this question and provide insights into maintaining privacy while leveraging the benefits of programmable payment systems. This informative journey as we uncover the impact of programmable payments on security and privacy prepares us to gain a comprehensive understanding of this technology's potential benefits and pitfalls [20].

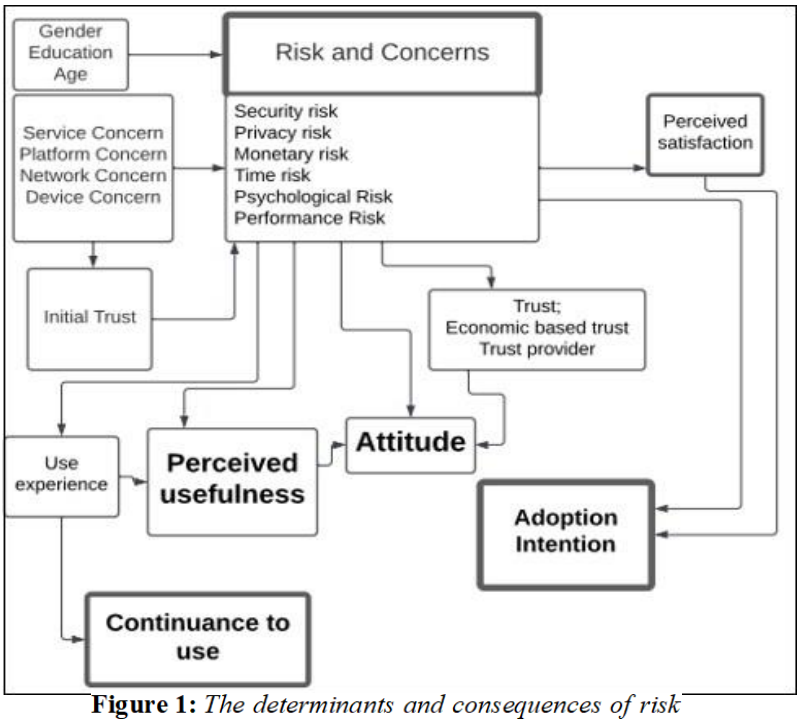

Figure 1: *The determinants and consequences of risk*

2. The Benefits of Programmable Payments

Programmable payments offer a range of benefits that make them an attractive option for businesses and individuals alike. One key advantage is the ability to automate transactions, reducing the need for manual intervention and streamlining the payment process [21]. This automation not only saves time but also minimizes the risk of human error, ensuring accurate and efficient transactions. Another benefit of programmable payments is the ability to customize payment flows and create rules for specific transactions [22]. This level of control allows businesses to tailor payment processes to their unique requirements, improving cash flow management and enhancing overall financial operations

[23]. In the ever-evolving landscape of programmable payments and blockchain technology, data protection emerges as a paramount concern [24]. These innovative financial solutions hold the potential to revolutionize the industry by enhancing efficiency, transparency, and cost-effectiveness. However, with the increasing volume of sensitive financial data being exchanged within these platforms, the security and privacy of this information become pivotal [25-26]. While blockchain technology offers cryptographic safeguards, it is not impervious to threats, necessitating robust data protection measures [27]. Ensuring the safeguarding of user data is not only an ethical obligation but a crucial element for gaining user trust, complying with emerging regulatory frameworks, and securing the sustainable growth of programmable payments. As regulatory authorities tighten their focus on this space, the onus is on industry stakeholders to implement and uphold stringent data protection practices, thus cementing programmable payments as a transformative force in the financial sector [28]. Additionally, programmable payments enable the integration of payment systems with other software applications, creating seamless and efficient workflows. Furthermore, programmable payments have the potential to enhance financial transparency [29-30]. By providing real-time access to transaction data, businesses can gain valuable insights into their financial health and make informed decisions. This increased visibility also fosters trust between parties involved in the transaction, as there is a clear record of every payment made [31]. While these benefits are undoubtedly compelling, it is crucial to address the security and privacy considerations associated with programmable payments.

3. The challenges of Programmable Payments in terms of Security and Privacy

With programmable payments becoming increasingly prevalent, the risks associated with security and privacy have become more pronounced. One of the main challenges is the potential for unauthorized access to sensitive financial information. Hackers are constantly evolving their tactics, and programmable payment platforms must remain vigilant in implementing robust security measures to protect against data breaches. Another challenge is the risk of fraudulent activities. Programmable payments involve the transfer of funds, making them an attractive target for cybercriminals. The challenges surrounding data protection in blockchain-based programmable payment systems underscore the intricate balance that must be struck between preserving the technology's fundamental characteristics, such as immutability and pseudonymity, and adhering to regulatory standards like GDPR, AML, and KYC [32]. Maintaining trust through blockchain's immutability while addressing the need for data correction and deletion in compliance with privacy regulations is a complex task. Similarly, pseudonymity, while safeguarding user privacy, presents hurdles in verifying user identities as required by financial regulations [33]. To navigate this complex landscape, innovative solutions, such as privacy-enhancing technologies and off-chain options, must be explored to ensure that the advantages of programmable payments are harnessed without compromising data protection, user privacy, and regulatory compliance. A thoughtful and well-balanced approach is essential to address these challenges successfully. Without adequate security measures in place, unauthorized transactions can occur, resulting in financial losses for businesses and individuals. In terms of privacy, programmable payments raise concerns regarding the sharing and storage of personal data. In the ever-evolving landscape of blockchain and cryptocurrency, safeguarding the security of smart contracts and payment systems is of paramount importance. Smart contracts, while offering automation and transparency, are not immune to vulnerabilities, and diligent measures such as security audits and code reviews are necessary to detect and address potential flaws before deployment. Moreover, the decentralized nature of these contracts can pose challenges in rectifying issues post-deployment, underscoring the importance of rigorous pre-deployment security protocols. Additionally, the integration of third-party services, although beneficial for enhancing functionality, can introduce security risks that demand thorough assessment and validation of the measures in place to protect user data and preserve the integrity of the entire payment system. In this dynamic environment, staying vigilant and proactive in ensuring the safety of these systems is the key to fostering trust and confidence among users and stakeholders. As transactions become more traceable, there is a need to ensure that individuals' privacy rights are respected. Additionally, the sharing of transaction data with various stakeholders, such as payment processors and regulatory authorities, raises questions about who has access to this information and how it is used. To address these challenges and mitigate

the risks, programmable payment platforms have implemented various security measures [34].

4. Overview of Security Measures in Programmable Payments

Programmable payment platforms recognize the importance of robust security measures to protect sensitive financial data. One of the primary security measures employed is encryption. By encrypting data during transmission and storage, programmable payment platforms ensure that unauthorized parties cannot access or decipher the information. Another security measure is multi-factor authentication. This involves verifying a user's identity through multiple factors, such as passwords, biometrics, or security tokens. By requiring multiple forms of authentication, programmable payment platforms add an extra layer of security, making it more difficult for unauthorized individuals to gain access to an account. Additionally, fraud detection and prevention systems are crucial in identifying and mitigating potential fraudulent activities. These systems use advanced algorithms and machine learning techniques to analyze transaction patterns, detect anomalies, and block suspicious transactions. While these security measures are effective in protecting against many common threats, there are still vulnerabilities that hackers can exploit [35].

5. Common Security Vulnerabilities in Programmable Payments

Despite the implementation of security measures, programmable payment platforms are not immune to security vulnerabilities. One common vulnerability is phishing attacks. Hackers may attempt to trick users into divulging their login credentials or other sensitive information through fraudulent emails or websites. Education and awareness are key in mitigating the risks associated with phishing attacks. Another vulnerability lies in the potential compromise of user devices. If a user's device is infected with malware or accessed by unauthorized individuals, sensitive financial information can be compromised. It is essential for users to keep their devices up to date with the latest security patches and employ antivirus software to minimize the risk of such compromises. Additionally, insider threats pose a significant risk to the security of programmable payment systems. Employees or individuals with authorized access to the platform may abuse their privileges or intentionally leak sensitive information [36-37]. Implementing strict access controls and regular monitoring can help mitigate the risks associated with insider threats. To further enhance security, there are best practices that both programmable payment platforms and users can adopt.

6. Best practices for Securing Programmable Payments

For programmable payment platforms, regular security audits and penetration testing are essential to identify and address vulnerabilities. By regularly testing their systems, platforms can proactively identify and address potential security weaknesses, ensuring the overall robustness of the payment infrastructure. Additionally, platforms should implement strong access controls and user authentication mechanisms. This includes enforcing password complexity requirements, implementing multi-factor authentication, and regularly reviewing and revoking access credentials for inactive or terminated users. For users of programmable payment systems, practicing good password hygiene is crucial. Using unique, complex passwords for each account and regularly changing them significantly reduces the risk of unauthorized access. Furthermore, users should exercise caution when sharing sensitive information and be vigilant for any suspicious activity or communications [38-39]. By adopting these best practices, both programmable payment platforms and users can enhance the security of their transactions and protect against potential threats.

7. The role of Privacy in Programmable Payments

While security measures are essential, it is also crucial to consider the privacy implications of programmable payments. As transactions become more traceable and information is shared with various stakeholders, individuals' privacy rights must be respected [40]. One aspect of privacy is the protection of personal data. Programmable payment platforms must adhere to data protection regulations and ensure that user data is collected, processed, and stored securely. This includes implementing measures such as data encryption, access controls, and regular audits to safeguard personal information. Another aspect of privacy is the transparency and control individuals have over their own financial data. Programmable payment platforms should provide individuals with clear information on how their data is used and shared and allow them to exercise control over the sharing of their information [41-42]. This includes providing options to opt out of certain data-sharing practices and allowing individuals to delete their data if they choose to do so. Striking the right balance between convenience and privacy is crucial in the realm of programmable payments.

8. Privacy Concerns and Solutions in Programmable Payments

As programmable payments become more prevalent, there are growing concerns regarding privacy. One

concern is the potential for unauthorized access to transaction data. While traceability can be beneficial for detecting and preventing fraudulent activities, it also means that transaction data is more susceptible to unauthorized access [43]. To address this concern, programmable payment platforms should employ strong encryption and access controls to ensure that only authorized individuals can access transaction data. Another privacy concern is the sharing of transaction data with third parties. While this sharing is often necessary for regulatory compliance and fraud prevention purposes, individuals should have control over how their data is shared. Programmable payment platforms can address this concern by providing clear opt-in and opt-out options for individuals, allowing them to choose which parties have access to their transaction data [44]. Regulatory frameworks also play a crucial role in protecting privacy in programmable payments.

9. Regulatory frameworks for Programmable Payments Security and Privacy

To ensure the security and privacy of programmable payment systems, regulatory frameworks have been established. These frameworks define the legal obligations and requirements that programmable payment platforms must adhere to. One such framework is the General Data Protection Regulation (GDPR) in the European Union [45]. The GDPR sets out guidelines and regulations for the collection, processing, and storage of personal data. Programmable payment platforms operating within the EU must comply with the GDPR to protect the privacy rights of individuals. the transformative potential of programmable payments harnessed through blockchain and cryptocurrencies, while also underscoring the significant security challenges associated with this innovation. One key concern is the susceptibility of smart contracts to coding errors and vulnerabilities, posing risks such as fund loss [46]. To mitigate these risks, the development community is actively engaged in regular security audits and stringent testing to bolster the security of smart contracts. Moreover, as the adoption of programmable payment platforms grows, so does their allure for cybercriminals, who target them with various threats, including DDoS attacks, phishing, and ransomware [47]. Robust cybersecurity measures, encompassing encryption, firewalls, and intrusion detection systems, are imperative to safeguard against these risks. It's worth noting that the blockchain and cryptocurrency space is evolving swiftly, with innovations like DeFi and NFTs introducing new dimensions to security challenges. Regulatory bodies and industry stakeholders are collaborating to establish frameworks and standards, further enhancing security and ensuring compliance. In essence, while programmable payments offer substantial benefits in terms of efficiency and cost-effectiveness, addressing security and privacy concerns is paramount to unlock the full potential of blockchain technology in the financial realm, necessitating continuous research and development to stay ahead of emerging threats and vulnerabilities. Additionally, regulatory bodies such as the Payment Card Industry Security Standards Council (PCI SSC) provide standards and guidelines for secure payment processing [48]. Compliance with these standards ensures that programmable payment platforms implement the necessary security measures to protect sensitive financial data. By adhering to these regulatory frameworks, programmable payment platforms can demonstrate their commitment to security and privacy [49].

10. Conclusion:

The future of programmable payments and its impact on security and privacy

Programmable payments have revolutionized the way we interact with money, offering unprecedented control and customization. However, the benefits of programmable payments must be balanced with the need for security and privacy. Despite the challenges and risks associated with programmable payments, the implementation of robust security measures and adherence to regulatory frameworks can mitigate these concerns. By prioritizing data encryption, multi-factor authentication, and fraud prevention systems, programmable payment platforms can protect against unauthorized access and fraudulent activities. In the realm of programmable payments enabled by blockchain technology and cryptocurrencies, a careful balance must be struck between the compelling benefits and the formidable challenges. The advantages are clear: automation enhances efficiency, blockchain's transparency fosters trust, and potential cost savings are on the horizon. However, these prospects are accompanied by a set of critical challenges. Security vulnerabilities in smart contracts and the constant threat of cyberattacks raise concerns, and the delicate equilibrium between transparency and user privacy must be carefully maintained. Regulatory compliance is essential to instill trust and encourage mainstream adoption. To navigate these challenges successfully, a multi-pronged approach is needed. Regular security audits, robust cybersecurity measures, user education, and the use of privacy-enhancing technologies such as zero-knowledge proofs and decentralized identity solutions are pivotal steps to ensure the long-term viability and widespread acceptance of programmable payments. By addressing these issues comprehensively, the potential of this transformative technology can be harnessed while safeguarding against its inherent risks. the critical significance of collaboration with regulatory authorities, strict adherence to Anti-Money Laundering (AML) and

Know Your Customer (KYC) requirements, and the proactive addressing of vulnerabilities in the realm of programmable payments. These measures are paramount for ensuring the integrity and security of this evolving financial ecosystem. By working closely with regulatory bodies, companies can maintain trust and legitimacy, while AML and KYC requirements serve as essential safeguards against illicit financial activities. Taking a comprehensive and collaborative approach that involves various stakeholders is advocated to tackle the unique challenges of programmable payments, bolstering security and reliability. This approach is pivotal in instilling confidence among users, investors, and regulators, thereby paving the way for programmable payments to revolutionize the finance industry, becoming a secure, efficient, and privacy-respecting payment system that reshapes the future of finance. Furthermore, by respecting individuals' privacy rights and providing transparency and control over the sharing of personal data, programmable payment platforms can foster trust and maintain privacy. As programmable payment systems continue to evolve, it is essential for businesses and individuals to stay informed about the latest security and privacy measures. By doing so, they can leverage the benefits of programmable payments while safeguarding their financial data and privacy. The potential of programmable payments, as we navigate the ever-changing landscape of security and privacy in the digital world. Programmable payments have emerged as a pivotal trend within the financial industry, revolutionizing the way customers interact with their finances. Bangor Savings Bank's adoption of programmable payments exemplifies how both smaller and larger banks are embracing this technology to offer a more personalized and convenient payment experience. With the ability to designate different funding sources for various transactions, customers gain unprecedented control and tailor their payment experience to suit their unique needs. This innovation is not only made possible through partnerships with financial technology leaders like Fiserv but also offers a cost-effective and seamless integration into existing card programs. In the ever-evolving payments landscape, programmable payments have become a competitive advantage, enabling financial institutions to meet the growing demand for flexibility and personalization while maintaining a prominent position in their customers' wallets.

References

[1] Teoh, W.M.Y.; Chong, S.C.; Lin, B.; Chua, J.W. Factors affecting consumers' perception of electronic payment: An empirical analysis. Internet Res. 2013, 23, 465–485.

[2] Sahi, A.M.; Khalid, H.; Abbas, A.F.; Khatib, S.F.A. The evolving research of customer adoption of digital payment: Learning from content and statistical analysis of the literature. J. Open Innov. Technol. Mark. Complex. 2021, 7, 230.

[3] De Luna, I.R.; Liébana-Cabanillas, F.; Sánchez-Fernández, J.; Muñoz-Leiva, F. Mobile payment is not all the same: The adoption of mobile payment systems depending on the technology applied. Technol. Forecast. Soc. Chang. 2019, 146, 931–944.

[4] Schierz, P.G.; Schilke, O.; Wirtz, B.W. Understanding consumer acceptance of mobile payment services: An empirical analysis. Electron. Commer. Res. Appl. 2010, 9, 209–216.

[5] Aljawder, M.; Abdulrazzaq, A. The effect of awareness, trust, and privacy and security on students' adoption of contactless payments: An empirical study. Int. J. Comput. Digit. Syst. 2019, 8, 669–676.

[6] Duane, A.; O'Reilly, P.; Andreev, P. Realising M-Payments: Modelling consumers' willingness to M-pay using Smart Phones. Behav. Inf. Technol. 2014, 33, 318–334.

[7] Kumar, A.S.; Arun Palanisamy, Y. Examining the consumers' preference towards adopting the mobile payment system. Int. J. Electron. Financ. 2019, 9, 268–286.

[8] Sorkin, D.E. Payment methods for consumer to consumer online transactions. Akron Law Rev. 2001, 35, 1–30.

[9] Hwang, J.J.; Yeh, T.C.; Li, J. Bin Securing on-line credit card payments without disclosing privacy information. Comput. Stand. Interfaces 2003, 25, 119–129.

[10] Qin, Z.; Sun, J.; Wahaballa, A.; Zheng, W.; Xiong, H.; Qin, Z. A secure and privacy-preserving mobile wallet with outsourced verification in cloud computing. Comput. Stand. Interfaces 2017, 54, 55–60.

[11] Kartika, H.; Fatimah, Y.A.; Supangkat, S.H. Secure Cashless Payment Governance in Indonesia: A Systematic Literature Review. In Proceedings of the 2018 International Conference on ICT for Smart Society (ICISS), Semarang, Indonesia, 10–11 October 2018; pp. 1–4.

[12] Yang, Y.; Liu, Y.; Li, H.; Yu, B. Understanding perceived risks in mobile payment acceptance. Ind. Manag. Data Syst. 2015, 115, 253–269.

[13] El Haddad, G.; Aimeur, E.; Hage, H. Understanding Trust, Privacy and Financial Fears in Online Payment. In Proceedings of the 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 28–36.

[14] Bagla, R.K.; Sancheti, V. Gaps in customer satisfaction with digital wallets: Challenge for sustainability. J. Manag. Dev. 2018, 37, 442–451.
[15] Kar, A.K. What Affects Usage Satisfaction in Mobile Payments? Modelling User Generated Content to Develop the "Digital Service Usage Satisfaction Model". Inf. Syst. Front. 2021, 23, 1341–1361.
[16] Grover, P.; Kar, A.K. User engagement for mobile payment service providers—introducing the social media engagement model. J. Retail. Consum. Serv. 2020, 53, 101718.
[17] Rahi, S.; Abd.Ghani, M.; Hafaz Ngah, A. Integration of unified theory of acceptance and use of technology in internet banking adoption setting: Evidence from Pakistan. Technol. Soc. 2019, 58, 101120.
[18] Luarn, P.; Lin, H.H. Toward an understanding of the behavioral intention to use mobile banking. Comput. Hum. Behav. 2005, 21, 873–891.
[19] Apanasevic, T.; Markendahl, J.; Arvidsson, N. Stakeholders' expectations of mobile payment in retail: Lessons from Sweden. Int. J. Bank Mark. 2016, 34, 37–61.
[20] Liu, R.; Wu, J.; Yu-Buck, G.F. The influence of mobile QR code payment on payment pleasure: Evidence from China. Int. J. Bank Mark. 2021, 39, 337–356.
[21] Singh, N.; Srivastava, S.; Sinha, N. Consumer preference and satisfaction ofM-wallets: A study on North Indian consumers. Int. J. Bank Mark. 2017, 35, 944–965.
[22] Uduji, J.I.; Okolo-Obasi, E.N. Young rural women's participation in the e-wallet programme and usage intensity of modern agricultural inputs in Nigeria. Gend. Technol. Dev. 2018, 22, 59–81.
[23] 23. Zhou, T.; Lu, Y.; Wang, B. Integrating TTF and UTAUT to explain mobile banking user adoption. Comput. Hum. Behav. 2010, 26, 760–767.
[24] Rahi, S.; Abd.Ghani, M. Investigating the role of UTAUT and e-service quality in internet banking adoption setting. TQM J. 2019, 31, 491–506.
[25] Al-Okaily, M.; Lutfi, A.; Alsaad, A.; Taamneh, A.; Alsyouf, A. The Determinants of Digital Payment Systems' Acceptance under Cultural Orientation Differences: The Case of Uncertainty Avoidance. Technol. Soc. 2020, 63, 101367.
[26] Putri, M.F.; Purwandari, B.; Hidayanto, A.N. What do affect customers to use mobile payment continually? A systematic literature review. In Proceedings of the 2020 Fifth International Conference on Informatics and Computing (ICIC), Gorontalo, Indonesia, 3–4 November 2020.
[27] Pramana, E. The Mobile Payment Adoption: A Systematic Literature Review. In Proceedings of the 2021 3rd East Indonesia Conference on Computer and Information Technology (EIConCIT), Surabaya, Indonesia, 9–11 April 2021; pp. 265–269.
[28] 28. Alkhowaiter, W.A. Digital payment and banking adoption research in Gulf countries: A systematic literature review. Int. J. Inf. Manag. 2020, 53, 102102.
[29] Boateng, R.; Sarpong, M.Y.P. A Literature Review of Mobile Payments in Sub-Saharan Africa; Springer International Publishing: Berlin/Heidelberg, Germany, 2019; Volume 558, ISBN 9783030206703.
[30] Wonglimpiyarat, J. Competition and challenges of mobile banking: A systematic review of major bank models in the Thai banking industry. J. High Technol. Manag. Res. 2014, 25, 123–131.
[31] Khatib, S.F.A.; Abdullah, D.F.; Hendrawaty, E.; Elamer, A.A. A bibliometric analysis of cash holdings literature: Current status, development, and agenda for future research. Manag. Rev. Q. 2021, 1–38, ahead of print.
[32] Hazaea, S.A.; Zhu, J.; Al-Matari, E.M.; Senan, N.A.M.; Khatib, S.F.A.; Ullah, S. Mapping of internal audit research in China: A systematic literature review and future research agenda. Cogent Bus. Manag. 2021, 8, 1938351.
[33] Zamil, I.A.; Ramakrishnan, S.; Jamal, N.M.; Hatif, M.A.; Khatib, S.F.A. Drivers of corporate voluntary disclosure: A systematic review. J. Financ. Report. Account. 2021, ahead of print.
[34] Hazaea, S.A.; Zhu, J.; Khatib, S.F.A.; Bazhair, A.H.; Elamer, A.A. Sustainability assurance practices: A systematic review and future research agenda. Environ. Sci. Pollut. Res. 2022, 29, 4843–4864.
[35] Block, J.H.; Fisch, C. Eight tips and questions for your bibliographic study in business and management research. Manag. Rev. Q. 2020, 70, 307–312.
[36] Khatib, S.F.A.; Abdullah, D.F.; Elamer, A.A.; Abueid, R. Nudging toward diversity in the boardroom: A systematic literature review of board diversity of financial institutions. Bus. Strateg. Environ. 2021, 30, 985–1002. [CrossRef]
[37] Abbas, A.F.; Jusoh, A.B.; Masod, A.; Ali, J. Market Maven and Mavenism: A Bibliometrics Analysis using Scopus Database. Int. J. Manag. 2020, 11, 31–45.
[38] Abbas, A.F.; Jusoh, A.; Mas'od, A.; Alsharif, A.H.; Ali, J. Bibliometrix analysis of information sharing in social media. Cogent Bus. Manag. 2022, 9, 2016556.
[39] Khatib, S.; Abdullah, D.F.; Elamer, A.; Hazaea, S.A. The Development of Corporate Governance Literature in Malaysia: A Systematic Literature

Review and Research Agenda. Corp. Gov. Int. J. Bus. Soc. 2022, ahead of print.
[40] Taylor, E. Mobile payment technologies in retail: A review of potential benefits and risks. Int. J. Retail Distrib. Manag. 2016, 44, 159–177. [CrossRef]
[41] Massaro, M.; Dumay, J.; Guthrie, J. On the shoulders of giants: Undertaking a structured literature review in accounting. Account. Audit. Account. J. 2016, 29, 767–801.
[42] Rasel, M.A.; Win, S. Microfinance governance: A systematic review and future research directions. J. Econ. Stud. 2020, 47, 1811–1847.
[43] 43. Khatib, S.F.A.; Abdullah, D.F.; Elamer, A.; Yahaya, I.S.; Owusu, A. Global trends in board diversity research: A bibliometric view. Meditari Account. Res. 2021, ahead of print.
[44] Khatib, S.F.A.; Abdullah, D.F.; Al Amosh, H.; Bazhair, A.H.; Kabara, A.S. Shariah auditing: Analyzing the past to prepare for the future auditing. J. Islam. Account. Bus. Res. 2022, ahead of print.
[45] Bürk, H.; Pfitzmann, A. Value exchange systems enabling security and unobservability. Comput. Secur. 1990, 9, 715–721.
[46] Mallat, N. Exploring consumer adoption of mobile payments—A qualitative study. J. Strateg. Inf. Syst. 2007, 16, 413–432.
[47] Dahlberg, T.; Mallat, N.; Ondrus, J.; Zmijewska, A. Past, present and future of mobile payments research: A literature review. Electron. Commer. Res. Appl. 2008, 7, 165–181.
[48] Slade, E.L.; Dwivedi, Y.K.; Piercy, N.C.; Williams, M.D. Modeling Consumers' Adoption Intentions of Remote Mobile Payments in the United Kingdom: Extending UTAUT with Innovativeness, Risk, and Trust. Psychol. Mark. 2015, 32, 860–873.
[49] Kim, C.; Tao, W.; Shin, N.; Kim, K.S. An empirical study of customers' perceptions of security and trust in e-payment systems. Electron. Commer. Res. Appl. 2010, 9, 84–95.