# Advance Journal of Econometrics and Finance
## Vol-4, Issue-2, 2026

**Advance Journal of Econometrics and Finance**

Online ISSN
2959-8990
Print ISSN
2959-8982
https://ajeaf.com/index.php/Journal/About

Name of Publisher: SCHOLAR CRAFT EDUCATION & RESEARCH HUB

Review Type: Double Blind Peer Review

Journal Frequency: Quarterly Research Journal (4- Issue)


# Digital Transformation in KSA: Assessing the Adoption of Blockchain and Smart Contracts under Vision 2030


[1]Muhammad Fahad Malik

**Muhammad Fahad Malik**
University of Prince Mugrin, Madinah, KSA.
Email: mo.malik@upm.edu.sa



**Abstract**

Background: Within the framework of Saudi Arabia's Vision 2030, the Kingdom is prioritizing digitalized citizen services, including secure e-government payment systems. However, adoption rates remain suboptimal due to factors related to user trust and technological familiarity. Hypothesis: This research tests the implications of blockchain-enforced identity management, smart contracts, and cybersecurity protocols on e-government payment adoption through the mediating role of perceived security of digital transactions. Methods: A quantitative study using structural equation modeling (SEM) in SmartPLS 4 was conducted with a sample of 500 Saudi Arabian citizens. Constructs were tested in terms of reliability, validity, and the mediation effect. Findings: Smart contract implementation had the most significant direct impact on adoption, followed by blockchain identity and cybersecurity protocols. Perceived security acted as a partial mediator in the adoption of smart contracts. The model demonstrated significant predictive power. Conclusion: Technological innovation alone is insufficient for mass adoption; it must be coupled with user trust. The study highlights that perceived security is the critical mechanism translating FinTech infrastructure into citizen adoption. These insights offer actionable guidance for policymakers and developers tasked with realizing the digital governance goals of Vision 2030.



**Keywords:** Blockchain, Cybersecurity, Digital Transformation, E-Government Payments, FinTech, Perceived Security, PLS-SEM, Saudi Vision 2030, Smart Contracts, Technology Adoption

## Introduction

Even though the Kingdom is currently undertaking massive digital transformation measures to align with the goals of Saudi Arabia's Vision 2030, the utilization of e-government payment systems remains suboptimal due to prevailing concerns regarding security, confidence, and system dependability (AlBliwi et al., 2025). Vision 2030 is an ambitious project attempting to revolutionize the public sector in Saudi Arabia, and e-government systems will be a major component of this revolution (Ali & Salih, 2025). One of the main aspects of this vision includes improving the security of e-government payments through the implementation of superior technologies, such as blockchain and financial technology (FinTech) (Altwijry et al., 2023).

Despite the promising potential to provide more secure digital payments, the effective use of technologies in FinTech platforms, such as blockchain-based identity management, smart contract implementation, and advanced cybersecurity protocols and their ability to impact citizen adoption is not yet fully understood (Alsakhnini & Almoaiad, 2024; Makki & Alqahtani, 2022). Blockchain technology integration is likely to offer effective identity management tools that support the verification and authentication procedures central to secure transactions (Alsakhnini & Almoaiad, 2024). Similarly, smart contract implementation can simplify the payments process through automation and by ensuring the rigorous execution of contracts, hence minimizing the chances of fraud and error (Shahid, 2025). A critical intervening variable that significantly impacts the degree of perceived security in digital transactions is the application of advanced cybersecurity measures within FinTech platforms (Khalid et al., 2025). The FinTech ecosystem in Saudi Arabia is evolving on a positive trajectory where the government, along with financial institutions, is investing extensively in technologies that can boost service access, efficiency, and security (Alhejaili, 2024). This strategy involves implementing multi-factor authentication, encryption algorithms, and AI-powered threat detection to ensure the protection of online transactions (Alshaikh et al., 2025). These measures align with the objectives of Vision 2030, striving to provide an environment that persuades the population to use and support e-government payment systems by facilitating a higher level of perceived security (AlBliwi et al., 2025).

However, there is a serious gap in the literature regarding the impacts of these technologies on the perceived safety of digital transactions, which acts as a key intermediary factor affecting user trust (Negm, 2024). Additionally, although these components have previously been discussed in isolated commercial environments, there are no systematic empirical studies examining the connectivity of these components within the public sector, particularly in the Saudi Arabian context (Alwadain et al., 2024). Qualitatively, most existing research is framed around case studies or theoretical reviews, which do not provide appropriate statistical modeling of causal relationships (Ali et al., 2025).

This constitutes a methodological gap that this study addresses using structural equation modeling (SEM). Addressing this issue is essential for developing safe, citizen-focused online platforms that contribute to greater acceptance and trust in governmental financial services (Ali et al., 2025). The objective of this study is to determine the impact of these emerging technologies on citizen perception of digital transaction security and, ultimately, on the adoption of government digital payment services (Negm, 2024). Finally, the evidence-based outcomes presented in this study provide actionable information for building safe, effective, and accessible e-government solutions, supporting the nation's aspirations for digitalization and the modernization of governance (Tiika et al., 2024).

## Literature Review

### Theoretical Lens

The theoretical framework used in this research is mainly anchored on the technology acceptance model (TAM) and the unified theory of acceptance and use of technology (UTAUT) as the theories of great power in the comprehension of user acceptance and uptake of emerging technologies. The usage of smart contracts supports safe financial operations, while the blockchain-based identity system provides a trustworthy procedure of authentication to contribute to the sense of technical integrity. Information assurance theory is applicable in the development of cybersecurity measures based on the belief that individuals are empowered by good security policies to trust online services. As a mediator variable, perceived security of digital transactions is grounded in trust-based models of technology adoption and has been determined to play a significant role in the behavior of users who act in risky situations like online payments. Finally, the use of e-government payment systems is a dependent variable theoretically conceptualized in the context of the TAM and the UTAUT. All these theoretical understandings provide a holistic view to examine how emerging technologies can persuade citizens to embrace secure online government systems.

### Theoretical Foundation

The measurement of this study is rooted in existing models of information systems, technology adoption, and digital trust to develop the roles and relationships between the variables employed in this research. The independent variables are based on the information systems success model and trust theory, which emphasize system quality, system

security, and system reliability as the key contributors to user trust and system adoption (DeLone & McLean, 2003; McKnight et al., 2002). The usage of smart contracts supports safe financial operations, while the system of blockchain-based identity provides a trustworthy procedure of authentication, which contributes to a sense of technical integrity. Information assurance theory is applied in the development of cybersecurity measures, founded on the belief that individuals are empowered by robust security policies and will consequently trust online services (Dhillon & Backhouse, 2001).

As a mediator variable, the perceived security of digital transactions is grounded in trust-based models of technology adoption and has been determined to play a significant role in the behavior of users who act in risky situations such as online payments (Gefen et al., 2003). Finally, the use of e-government payment systems is a dependent variable theoretically conceptualized in the context of the TAM and the UTAUT (Venkatesh et al., 2022). According to these models, the outcome of the behavioral intentions of users depends on performance expectations, perceived usefulness, and trust in the system. All these theoretical understandings provide a holistic view that can be used to examine how emerging technologies can persuade citizens to embrace secure online government services.

**Blockchain Identity Management:** In the near future, identity is a system built on blockchain. Blockchain identity management refers to identity verification, authentication, and digital management by a decentralized ledger technology that offers high security and accuracy in identity management. When compared to a centralized system, one can acquire an identity in blockchain that gives them credentials that are encrypted, immutable, and traceable, making identity theft and unauthorized access far more difficult (Rahman et al., 2024). The e-government payment case involves using this technology to design trust at the base layer; this approach provides the user with increased control because the verification of identities would be more transparent (Zhang & Alghamdi, 2023).

The significant shift of the identity management concept toward more secure and decentralized forms fueled by blockchain technology has entailed changing anchored paper-based and centralized digital systems. To begin with, the digital identity systems used were grounded on centralized databases, which opened up significant vulnerability to the risk of data disclosure and failure. With the growing popularity of blockchain in the early 2010s, scholars began research on decentralized identity (DID), where identity credentials are controlled by individuals themselves without having to work with a middleman (Zyskind et al., 2015). This eventually evolved into self-sovereign identity systems, which offer privacy-preserving and cryptographically secure authentication protocols (Allen, 2016). Later definitions of identity have focused more on blockchain-based identity as a verifiable, user-friendly, and interoperable system that facilitates trust and efficiency in web-based government services (Rahman et al., 2024).

The field of cyber governance points toward research into identity management facilitated by blockchains because credible and secure identity authentication is a pillar of delivering trusted e-government services. Traditional forms of identity systems are centralized and more susceptible to fraud, identity crimes, and unauthorized access, which may compromise citizen data and the confidence of the population (Rahman et al., 2024). User-sovereign authentication with blockchain can enhance privacy and transparency due to decentralized and immutable identity authentication (Zhang & Alghamdi, 2023). This idea may be interpreted to develop safe and user-friendly foundations that align with Vision 2030. Failure to stay focused on these measures can lead to exposed data and a failure to adopt the technology, ultimately causing digital transformation efforts to fail (Alotaibi & Alkhalifah, 2023).

**Smart Contracts Payments:** Smart contracts are self-executing agreements that are automatically enforced on a blockchain platform when predefined conditions are met. Within e-government systems, they are utilized for taxation and the payment of services, regulating activities while removing manual procedures and third-party intermediaries (Alotaibi & Alkhalifah, 2023). Their transparency and immutability ensure transaction integrity and reduce processing delays, which instills trust in citizens and maximizes the efficiency of state financial services (Khalid et al., 2025).

Programmable contracts, often referred to as smart contracts, were first conceptualized in the 1990s by Szabo (1997), who envisioned them as a way to automatically execute contract terms without intermediaries. While initially a theoretical concept, practical implementation emerged around 2015 with the rise of blockchain platforms like Ethereum. Early definitions focused on the ability to facilitate automated transactions within financial systems, particularly cryptocurrency exchanges. Over time, the application of smart contracts has expanded to encompass complex multi-party agreements in domains such as supply chains, insurance, and governance (Christidis & Devetsikiotis, 2016). The public sector now views smart contracts as a means of automating secure payments and enhancing transparency, thereby reducing manual errors in service delivery (Zhang & Alghamdi, 2023).

The implementation of smart contracts is a subject of critical investigation, as these self-executing applications automate payment systems, minimize human error, and optimize procedural design. Smart contracts benefit e-government by increasing efficiency in service provision, reducing corruption, and enhancing accountability by ensuring that payments are released only when specific terms are satisfied (Khalid et al., 2025). When integrated properly, they significantly improve user trust and satisfaction with

governmental services. Conversely, a lack of smart contract integration may leave public systems ineffective, prone to errors, and lacking the transparency necessary to drive user engagement and operational efficiency (Zhang & Alghamdi, 2023).

**Fintech Cyber Protection:** FinTech cybersecurity involves technical and organizational solutions designed to guarantee the safety of financial data and software environments; these include encryption, multi-factor authentication, intrusion detection systems, and continuous surveillance (Hussein & Yousef, 2024). In e-government payment systems, robust cybersecurity practices ensure that the sensitive personal information of citizens and state financial resources are safeguarded. These measures serve as critical determinants of the trust users place in the system and their subsequent decision to adopt digital payment methods (Khalid et al., 2025).

The digitization of financial services has prompted a significant shift in cybersecurity, moving beyond the traditional firewalls and antivirus software previously used to protect IT infrastructure. At the beginning of the 21st century, cybersecurity in FinTech was primarily concerned with network security. As threats evolved, the focus expanded to encompass end-to-end encryption, biometric authentication, and real-time fraud detection systems (ENISA, 2016). With the rising momentum of FinTech, the definition has grown to include comprehensive frameworks that protect digital resources, ensure regulatory compliance, and maintain user data ownership within cloud-based and decentralized operations. Today, FinTech cybersecurity is characterized not only by technical protection mechanisms but also by AI-managed threat detection and cross-border data management (Khalid et al., 2025).

Cybersecurity measures for FinTech platforms are vital to investigate due to the high risks associated with online financial systems. These platforms are primary targets for cyberattacks, data breaches, and service disruptions, especially as e-government services increasingly depend on FinTech infrastructure (Hussein & Yousef, 2024). Features such as advanced encryption, proactive threat detection, and rigorous access control are essential for building resilient systems that protect citizen information and provide the confidence necessary to trust e-government services (Khalid et al., 2025). Failure to prioritize these aspects can result in financial loss, legal repercussions, and a decline in public confidence in government-led online services (ENISA, 2023).

**Perceived Dealings Cybersafety:** Perceived security of internet transactions refers to the degree of confidence that individuals feel regarding the safety of their financial and personal details during online transactions. It reflects the belief that digital platforms can effectively prevent fraud, abuse, and unauthorized access (Gefen et al., 2003; Hussein & Yousef, 2024). Within the context of e-government payments, security perception is a leading force behind user confidence and adoption, particularly as cybersecurity awareness and sensitivity to privacy threats continue to grow.

The concept of perceived security emerged in the late 1990s as e-commerce gained momentum, leading scholars to investigate how system safety perceptions impact online purchase behavior (Gefen et al., 2003). Originally conceptualized as a safeguard against credit card fraud and data abuse, the idea has evolved alongside digital service ecosystems. With the development of mobile banking, FinTech, and e-government services, perceived security now encompasses broader dimensions, including privacy guarantees, transparency, and user control over personal information. Modern conceptualizations view perceived security as a multidimensional variable incorporating technical, behavioral, and psychological factors that influence trust and technology acceptance, especially in sensitive digital dealings (Hussein & Yousef, 2024).

Citizen behavior is central to the adoption of digital government platforms and requires fundamental trust in security. Regardless of the objective effectiveness of a system, how users perceive the handling of their personal and financial data strongly influences their adoption of e-payment services (Gefen et al., 2003; Hussein & Yousef, 2024). Cultivating perceived security in public online services helps reduce resistance to change and allows designers and policymakers to align technical functionality with user expectations. Failure to address perceived security can lead to public cynicism, low adoption rates, and diminished returns on technological investments (Rahman et al., 2024).

**E-Government Payments:** The adoption of e-government payment systems involves the intent to use and the actual utilization of electronic government platforms for financial matters, such as taxation and the payment of utility or licensing fees. Factors influencing this adoption include perceived usefulness, ease of use, social influence, and perceived security (Venkatesh et al., 2022). Within the framework of Saudi Vision 2030, the successful implementation of these systems serves as a primary indicator of digital transformation and the modernization of the public sector (Alotaibi & Alkhalifah, 2023; UN E-Government Survey, 2022).

The acceptance of e-government services has evolved from early considerations of internet accessibility and digital literacy in the early 2000s to comprehensive models that emphasize attitudes, trust, and the impact of system quality on the user. While access and basic functionality were initial determinants, modern digital platforms require a nuanced understanding of behavioral intention, usability, personalization, and perceived value (Carter & Bélanger, 2005). For online payments, the willingness of citizens to engage with government services depends on security, convenience, and transparency. Recent academic definitions have incorporated institutional trust, digital maturity, and policy fit, which are particularly relevant for rapidly digitizing nations like Saudi Arabia (Alotaibi & Alkhalifah, 2023; Venkatesh et al., 2022).

The integration of e-government payment systems is an essential factor in determining the success of digital public service initiatives. It represents an attitude–behavior hybrid used to assess how individuals embrace and utilize technology to complete transactions with the government (Venkatesh et al., 2022). This behavior can be analyzed to uncover adoption barriers, such as usability issues, low trust, or a lack of perceived value (Alotaibi & Alkhalifah, 2023). High adoption rates lead to increased transparency, improved governance, and cost efficiency. Conversely, poor adoption dynamics can result in underutilized systems and the failure to achieve national digital transformation goals (UN E-Government Survey, 2022).

**Hypotheses Development**

Blockchain-based identity management is considered a revolutionary application of credible authentication in online government services. Unlike centralized identity systems that are vulnerable to data breaches and single points of failure, blockchain provides decentralization, which ensures transparency, immutability, and user control over identity information. These properties significantly reduce the risks of fraud and theft, assisting citizens who intend to rely more on government facilities. Reliable identification is essential for e-government payments because financial transactions must be supported by the verified identity of legal subjects. Recent studies indicate that blockchain-based identity solutions positively influence user trust and confidence, thereby increasing the willingness to utilize e-government services (Rahman et al., 2024; Zhang & Alghamdi, 2023).

Furthermore, blockchain identity solutions align with national digital transformation plans, as the Saudi Arabia Vision 2030 is built on the foundations of safe and people-focused services. Self-sovereign identity reduces the need for third-party verifiers, enabling faster and safer interactions with e-government systems. This leads to higher user confidence, improved efficiency, and increased system transparency, which are fundamental drivers of technology adoption (Alotaibi & Alkhalifah, 2023). Recent empirical evidence suggests that blockchain identity solutions support higher acceptance of online financial services, particularly where privacy and security are critical factors (Hussein & Yousef, 2024; Khalid et al., 2025). Consequently, the implementation of blockchain-based identity management is expected to enhance the use of e-payment systems in government by mitigating the primary barriers of security and trust in digital identity.

**H1: Identity management that uses blockchain has a positive and significant impact on the adoption of e government payment systems.**

The introduction of smart contracts represents another fundamental application of blockchain technology, providing a safe, transparent, and automated method for conducting transactions. The use of smart contracts in e-government payment procedures is associated with a decrease in human contact and the reduction of potential errors, as payments are only released upon the completion of predetermined conditions. This automation ensures that transactions are verified and irrevocable, thereby reducing corruption and enhancing the accountability of government services (Zhang & Alghamdi, 2023). Most citizens adopt digital government platforms when they believe that transactions are conducted in an objective manner, free from manipulation. Empirical data suggest that smart contract-based payment systems improve transaction efficacy while developing trust in government-run digital services, which serves as a primary motivating factor for adoption (Rahman et al., 2024).

Furthermore, the introduction of smart contracts aligns with the long-term agenda of national digital transformation, including Saudi Vision 2030, which aims for efficient, citizen-centered, and secure public services. Smart contracts ensure that e-government payment systems are usable and reliable by omitting middlemen and reducing management costs. Research indicates that these systems record high measures of user satisfaction and adoption intention (Hussein & Yousef, 2024). Additionally, the use of smart contracts supports compliance with governmental laws, guaranteeing consistent service quality and fostering greater reliance on digital tools (Khalid et al., 2025). Therefore, it is assumed that the implementation of smart contract technology will positively and substantially affect the readiness of citizens to adopt e-government payment systems, serving as an essential trigger for effective digital governance initiatives.

**H2: Smart contract implementation for payments has a positive and significant effect on e government payment system adoption.**

Building trust in online financial services, particularly within e-government payment systems where sensitive personal and financial data are exchanged, is fundamentally based on cybersecurity regulations. These systems employ potent security controls such as encryption, intrusion detection, and multi-factor authentication measures to prevent data theft and fraudulent cyberattacks. Once citizens believe that government payment systems possess adequate cybersecurity, they are more likely to adopt and actively utilize these platforms (Hussein & Yousef, 2024). Research within the FinTech industry demonstrates that cybersecurity provisions do not merely address technical vulnerabilities but directly influence adoption modes by increasing the tiers of trust and confidence in virtual platforms (Rahman et al., 2024). Consequently, cybersecurity practices are not just technical tools but are essential for the ability of citizens to engage with digital governance systems.

In the context of Saudi Arabia Vision 2030, the implementation of cybersecurity practices is a national priority aimed at creating a safe internet environment that supports innovation and citizen interaction. When governments integrate advanced security protocols such as AI-based threat detection systems and blockchain-based security solutions, it becomes possible to maintain stable and reliable e-payment systems capable of withstanding various cyberattacks (Khalid et al., 2025). Studies indicate that a primary reason citizens avoid e-services is the absence of adequate cybersecurity, and comprehensively designed policies can significantly contribute to service adoption (Alotaibi & Alkhalifah, 2023). This demonstrates that cybersecurity controls have a positive and direct impact on e-government payment systems adoption because they lower perceived risks and protect the continuity of digital services.

**H3: Cybersecurity protocols on FinTech platforms have a positive and significant impact on the adoption of e government payment systems.**

Building trust in online financial services, particularly within e-government payment systems where sensitive personal and financial data are exchanged, is fundamentally based on cybersecurity regulations. These systems employ potent security controls such as encryption, intrusion detection, and multi-factor authentication measures to prevent data theft and fraudulent cyberattacks. Once citizens believe that government payment systems possess adequate cybersecurity, they are more likely to adopt and actively utilize these platforms (Hussein & Yousef, 2024). Research within the FinTech industry demonstrates that cybersecurity provisions do not merely address technical vulnerabilities but directly influence adoption modes by increasing the tiers of trust and confidence in virtual platforms (Rahman et al., 2024). Consequently, cybersecurity practices are not just technical tools but are essential for the ability of citizens to engage with digital governance systems.

In the context of Saudi Arabia Vision 2030, the implementation of cybersecurity practices is a national priority aimed at creating a safe internet environment that supports innovation and citizen interaction. When governments integrate advanced security protocols such as AI-based threat detection systems and blockchain-based security solutions, it becomes possible to maintain stable and reliable e-payment systems capable of withstanding various cyberattacks (Khalid et al., 2025). Studies indicate that a primary reason citizens avoid e-services is the absence of adequate cybersecurity, and comprehensively designed policies can significantly contribute to service adoption (Alotaibi & Alkhalifah, 2023). This demonstrates that cybersecurity controls have a positive and direct impact on e-government payment systems adoption because they lower perceived risks and protect the continuity of digital services.

**H4: Perceived security of digital transactions mediates the relationship between blockchain enabled identity management and e government payment system adoption.**

Blockchain-based identity management provides decent technical security against fraud and unauthorized access, but it generally depends upon the perceived system security of the citizens. Even though one can assume that blockchain is immutable and decentralized when it comes to verification, such technical aspects must be converted into user trust in order to facilitate prolific use. Perceived security is the psychological relationship between the capabilities of the technology and the willingness of the users to be enrolled in e-government payment systems. It has been stated that without a certain level of sophistication, none of the systems of identity may be trusted by citizens, and this gives it an impossible task to find safety (Gefen et al., 2003; Hussein & Yousef, 2024). That is why identity on blockchain will positively affect adoption indirectly, through positive perceptions of digital security, which, in turn, influence the behavioral intentions of the users. Research by others confirms that the success of perceived security is an important factor in the relationship between technological enabling factors and system adoption in terms of e-government, especially in the developing and transitional economies like Saudi Arabia (Rahman et al., 2024; Alotaibi & Alkhalifah, 2023).

Blockchain-facilitated identity can be alive to its potential only when perceived as providing the citizens with a sense of security and when the citizens believe that their personal and financial information is being kept safe. When users feel that they have the protection of their identities in the form of blockchain, they are assured that they can safely afford to pay digital cash to state agencies, which can lead to more users taking up blockchain. Therefore, one of the key mediating factors is perceived security since the adoption outcome will be only correctly illustrated by the reality of the actual results of the blockchain-aided identity management technical strengths (Khalid et al., 2025).

**H5: Perceived security of digital transactions mediates the relationship between smart contract implementation for payments and e-government payment system adoption.**

The idea behind smart contracts is that they reduce reliance on middlemen; such agreements require the execution of transactions automatically in accordance with rules established in advance, which enhances transparency and removes the risk of manipulation. However, the effectiveness with which smart contracts encourage citizens to use e-government payment systems is strongly dependent on the level of trust that users have in the system. Even though the principles of smart contracts suggest integrity and compliance, residents are only willing to operate such systems if they believe their payments are being made securely and fairly. Consequently, perceived security is one of the

key psychological motivations connecting the performance and automation of smart contracts to the behavioral intention of adopting digital payment systems (Hussein & Yousef, 2024; Zhang & Alghamdi, 2023).

Non-adoption may occur when positive perceptions of security are absent despite the availability of technologically advanced solutions. Recent studies on the adoption of FinTech and e-government reveal the impact of perceived security on adoption intentions and user trust regarding technological innovations (Khalid et al., 2025; Rahman et al., 2024). Where digital trust constitutes a significant component of Vision 2030 reforms, such as in Saudi Arabia, the implementation of smart contracts can be effective only when individuals believe that their dealings are safe, transparent, and resistant to fraud. This mediation effect is considered specifically because, even though smart contracts are technically reliable, citizens who are not well-versed in blockchain actions are likely to doubt their validity. In addition to providing a sense of security in transactions, smart contracts facilitate the buildup of trust and confidence, leading to a smoother transition toward e-government payment systems (Alotaibi & Alkhalifah, 2023).

**H6: Perceived security of digital transactions mediates the relationship between FinTech cybersecurity protocols and e government payment system adoption.**

The implementation of robust cybersecurity practices is a technical necessity that significantly shapes the psychological perception of safety among users of digital platforms. While technical measures like encryption and threat detection provide the mechanical shield for data, it is the user perception of these measures that ultimately drives the decision to adopt e-government payment systems. Perceived security acts as a mediating bridge because even the most advanced cybersecurity protocols cannot guarantee adoption if citizens do not perceive the system as trustworthy and safe from fraud (Hussein & Yousef, 2024). Within the digital landscape of Saudi Arabia, the transition to online financial dealings is heavily influenced by how effectively cybersecurity measures reduce the perceived risk of privacy breaches and financial loss (Khalid et al., 2025).

Research indicates that the relationship between cybersecurity efforts and user behavior is not always direct; rather, the confidence instilled by these protocols creates a fertile ground for technology acceptance (Rahman et al., 2024). When individuals observe visible security indicators, such as biometric authentication or AI-managed monitoring, their perceived security increases, which in turn reduces resistance to e-government services (Alotaibi & Alkhalifah, 2023). Therefore, the impact of cybersecurity on adoption is partially explained by its ability to enhance the subjective feeling of safety among the population (Khalid et al., 2025). Without this mediation of perceived security, technical security measures might be viewed as complex barriers rather than facilitators of digital trust (ENISA, 2023).

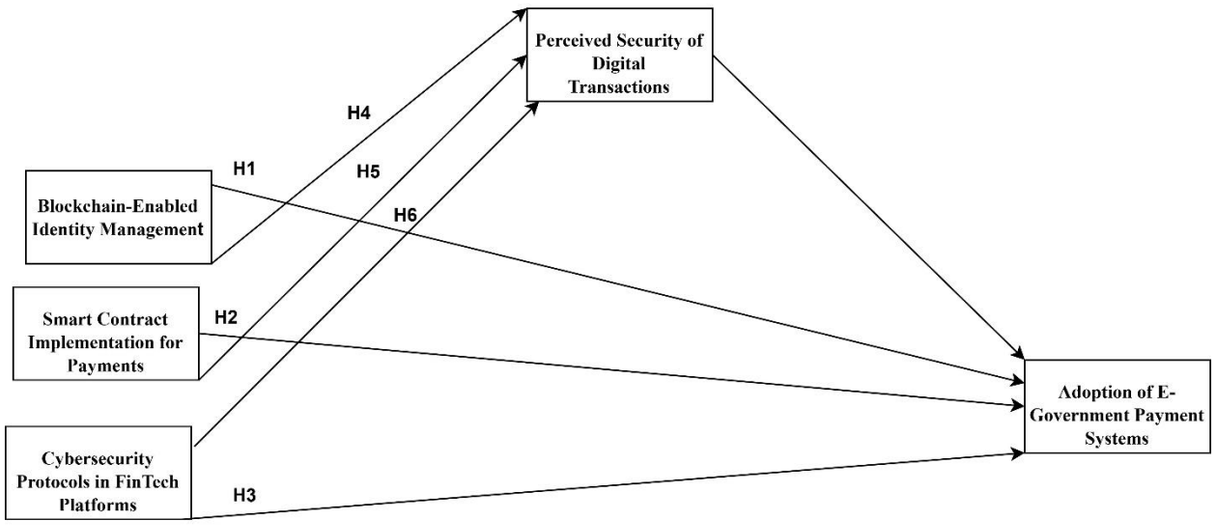


***Figure 1: Research Proposed Model***

## Methodology

### Research Design

The current study utilizes a cross-sectional survey research design and a quantitative approach to examine the relationships between blockchain-based identity management, smart contract implementation, cybersecurity practices, perceived digital transaction security, and the adoption of e-government payment systems. A survey-based design is appropriate as it allows for the collection of substantial primary data to test hypothesized associations using a structural equation modeling (SEM) framework (Hair et al., 2022). Partial least squares structural equation modeling (PLS-SEM), supported by SmartPLS 4, was selected because it is particularly robust for predictive research questions, models involving mediation, and studies in nascent fields such as full-scale FinTech adoption in e-government (Sarstedt et al., 2023).

Advance Journal of Econometrics and Finance
Vol-4, Issue-2, 2026

**Population and Sampling**

The population of interest for this study consists of citizens and residents of Saudi Arabia who have experience using or accessing e-government payment systems. The sample size was established at 500 respondents to ensure generalizability and statistical power; this figure exceeds the "10 times rule" the requirement that a sample be at least 10 times the maximum number of structural paths directed at a particular construct in the PLS path model (Hair et al., 2022). Purposive sampling was employed to target members of the general public who have specifically engaged with digital government payment services. This approach ensures the data remains germane to citizen behavior and instrumental in confirming the research findings.

**Respondents' Profile**

The study collected demographic and institutional data to provide context for the findings. The sample of 500 participants comprised 52% males and 48% females. The age of the respondents ranged from 20 to 55 years, with the highest proportion (40%) falling between the ages of 26–35 and 36–45. This indicates high participation from the working-age population most actively engaged in digital services.

The sample consists entirely of the general public, including private-sector employees (45%), self-employed individuals (25%), students (15%), and other residents utilizing e-government systems (15%). Regarding functional engagement, 40% of respondents utilized platforms related to municipal and financial affairs, 30% engaged with digital transformation and ICT services, and 30% were general users of various e-government portals. This distribution ensures a diversity of perspectives across different categories of public users and enhances the representativeness of the results concerning citizen adoption (Hussein & Yousef, 2024).

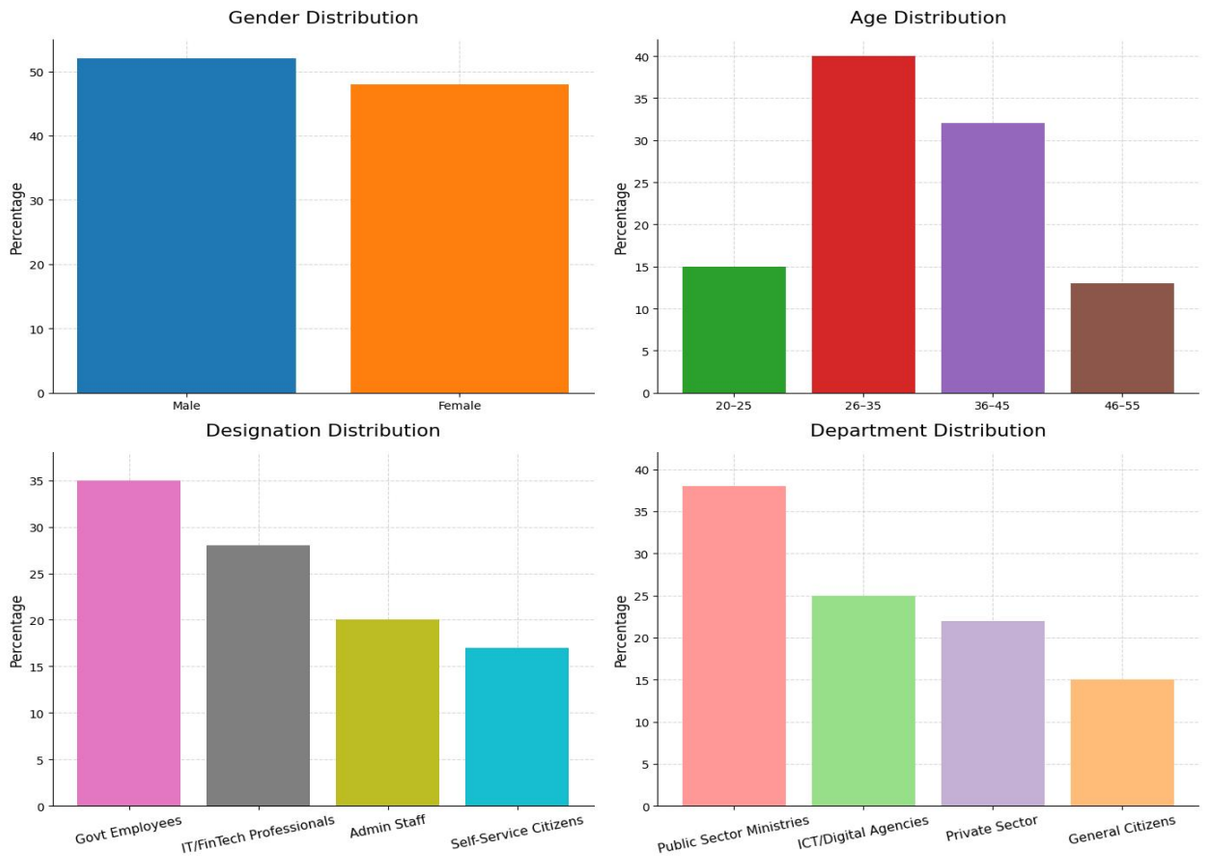


***Figure 2: Respondents Profile***

**Data Collection Instruments**

Data were collected using a structured questionnaire on a five-point Likert scale (1 = *Strongly disagree*, 5 = *Strongly agree*) that was used to test conceptually the conceptual framework. The adaption of the instruments that had been validated previously was reflected in the measurement of each construct on different items of the academic literature. Six indicators were employed to assess blockchain-enabled identity management, based on the study by Zwitter and Boisse-Despiaux (2020) and Al-Sharafi et al. (2022), and became decentralization, integrity of data, authentication of users, the resistance to entities fiddling, transparency, and control of users. The smart contract implementation payments comprises seven questions that aim to provide answers to the automatic execution, terms transparency, cost-efficiency, speed of financings, irreversibility, and reduction of errors, according to Hasan et al. (2021). ENISA (2019) and Alarifi et al. (2020) recommend that evaluation of FinTech platforms cybersecurity protocols involves

seven items (encryption, multi-factor authentication, adherence to the threats posed by data protection regulations, incident recovery measures, system vulnerability management, and real-time monitoring of threats).

Five items based on Pavlou and Deng (2003) and Deng et al. (2010) measured perceived security of digital transactions with user perception of the system: data safety, fraud protection, quality of the encryption, secure access control, trust in the system, and confidentiality of the transactions. Finally, there was adoption of e-government payment systems which used six items on intention to use, system accessibility, system reliability, perceived usefulness, satisfaction with use, and continued use as indicated by Venkatesh et al. (2003) and Shareef et al. (2011). Pilot-testing has been utilized to check the clarity of the test and reliability and to be certain that all the variables were highly internalized with Cronbach's alpha values being higher than the acceptable level of 0.70.

**Data Analysis**

Collected data have been analyzed using SmartPLS 4 that calculates a variance-based SEM that can be used when the model under analysis includes mediation effects and that the constructs are mostly multidimensional (Sarstedt et al., 2023). The test was carried out in two phases: measurement with the analysis of reliability, convergent, and discriminant validity; structural analysis with verification of the assumptions and the associations using the path (Hair et al., 2022). The mediation check was determined to examine the role of perceived security in the association among the independent variables and adoption of e-government payment systems in line with the bootstrapping techniques proposed in the PLS-SEM literature.

**Common Method Bias**

This paper uses procedural and statistical remedies to eliminate the common biases on the method (CMB) that results where measurement error is assumed to arise because of the measuring tool and none of the construct measures. Procedurally, the anonymity and confidentiality were ensured and assessment apprehension and social desirability effects were reduced. The questions were formulated positively and were distributed across the questionnaire sections so as to discourage the chance of giving patterned answers. To determine the presence of CMB, the single factor test, which is Harman's single-factor test was taken to determine the presence of only one factor that can describe a significant portion of the variance. Harman's one-factor tests showed common method bias was not present, as the first factor accounted 39.80% of the variance, which is not greater than critical value of 50% (Podsakoff et al., 2003).

**Assessment of Measurement Model**

Data analysis was done using the Partial Least Squares (PLS) as a combination of two data analysis methods considering the variance analysis and structural equation modeling (SEM). The results were analyzed with the help of SmartPLS 4 (Ringle et al., 2024). Hair et al. (2009) contend that SEM is quite appropriate when the research includes over two variables and constructs as it facilitates establishing relationships simultaneously. In addition, the PLS-SEM is superior to CB-SEM in ascertaining the predictive power of the model (Hair et al., 2016). A measurement model evaluation was conducted by, first of all, examining the loading of the factor and internal consistency reliability.

Table 1 evaluates internal consistency, reliability, and convergent validity of three constructs Adoption of E-Government Payment Systems (AEPS), Blockchain-Enhanced Identity Management (BEIM), and Smart Contract Implementation of Payments (SCIP) and five (in rows) constructs of payment security propositions compared to FinTech Platform (CPFP) and Received Security of digital transactions (PSDT) as a structural equation modeling (SEM) model. All the constructs meet the required standards of Cronbach's alpha (0.70 and above) and Composite Reliability (CR 0.70 and above) and display high-level of internal consistency and construct reliability (Hair et al., 2010; Nunnally & Bernstein, 1994). AEPS and SCIP are more precisely good (0.962 each) in terms of CR. In addition, the AVE of each of the constructs is greater than 0.50 which is recommended convergence validation (Fornell & Larcker, 1981). Factor loading of the individual indicators is usually greater than 0.70 which implies the significance of an item to the respective constructs. BEIM boasts the lowest AVE (0.575) and therefore validity - AEPS boasts the best convergent validity (AVE = 0.810). All these operations affirm the validity of the measurement model and promise that the latent measures are reliable and valid in the framework of adoption of e-government payment systems.

Table 2 demonstrates Heterotrait-Monotrait (HTMT) ratio of constructs, as an instrument, which is effective to determine the specificity of latent variables. All constructs have acceptable discriminant validity between the constructs, indicated by all values of HTMT that fall below a conservative cut of 0.85, a recommendation of Henseler et al. (2015). The highest score of HTMT is observed between BEIM (Blockchain-Enabled Identity Management) and SCIP (Smart Contract Implementation for Payments) with a median of 0.676 that is medium but fails to reflect serious differentiation. AEPS (Adoption of E-Government Payment Systems) values when compared to the other constructs are 0.456 to 0.555 which suggest that it is conceptually different in that it passes through the model. Also contributing to the discriminant validity of the measurement model are

the relatively low scores of CPFP (Cybersecurity Protocols in FinTech Platforms), PSDT (Perceived Security of Digital Transactions) and the other constructs. In most cases, these findings confirm that the constructs are distinct and they do not engage each other concerning their contribution to the theoretical understanding.

The Variance Inflation Factor (VIF) of single measurement items which was utilized to quantify the multicollinearity between indicators within each construct is presented in Table 3. A VIF 2.0–5.0 value is an indication of reasonable level of collinearity that implies that multicollinearity does not exist in this model (Hair et al., 2010). All items of the five constructs of AEPS (Adoption of E-Government Payment Systems) of BEIM (Blockchain-Enabled Identity Management) of CPFP (Cybersecurity Protocols in FinTech Platforms) of PSDT (Perceived Security of Digital Transactions) and SCIP (Smart Contract Implementation for Payments), VIF is between 2.812 and 4.188. VIF is highest in the AEPS6 (4.188) and lowest in the SCIP6 (2.812): whichever the case remains within the acceptable level. These findings indicate that there is no problem of multicollinearity, and they support the consistency and robust prediction of estimated path coefficients of the structural model.

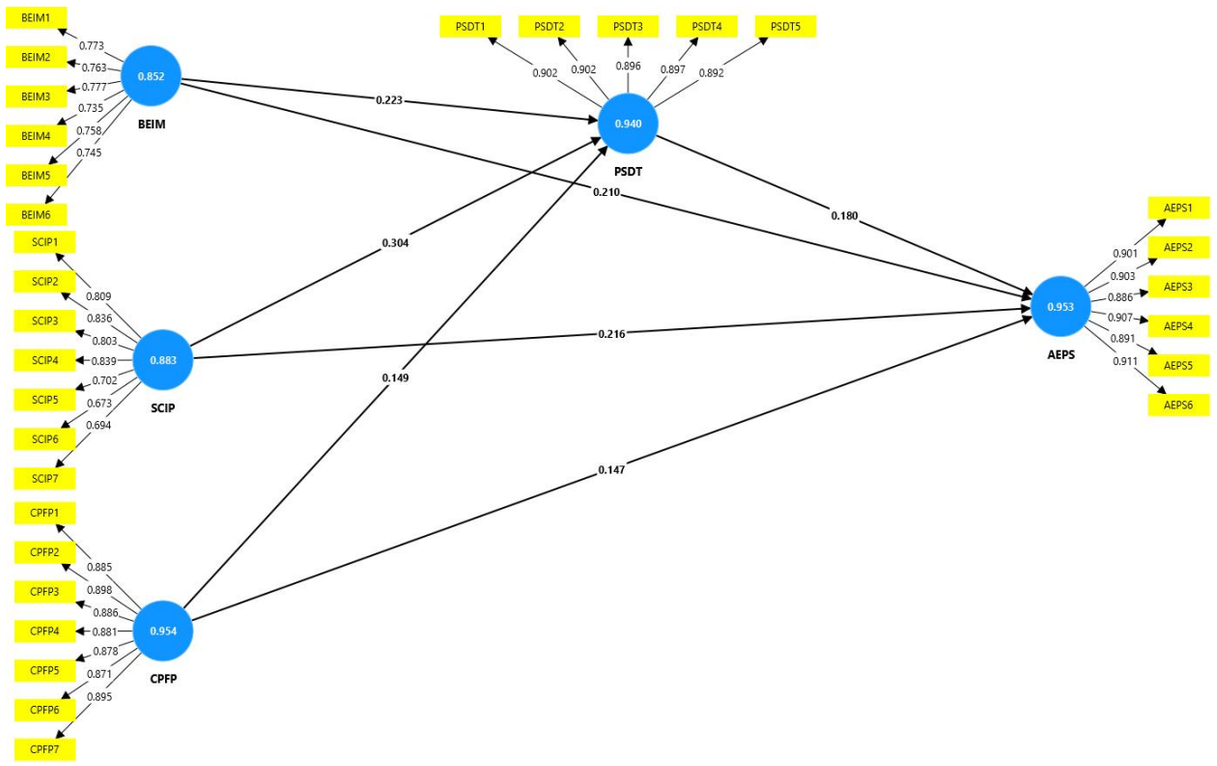


*Figure 3: SEM with Factor Loadings and Alpha Values of Variables*

**Table 1:** *Internal Consistency, Reliability and Convergent Validity*

| Construct | Indicator | Factor Loading | Cronbach's Alpha | Composite Reliability | Average Variance Extracted (AVE) |
|---|---|---|---|---|---|
| AEPS | AEPS1 | 0.901 | 0.953 | 0.962 | 0.810 |
| | AEPS2 | 0.903 | | | |
| | AEPS3 | 0.886 | | | |
| | AEPS4 | 0.907 | | | |
| | AEPS5 | 0.891 | | | |
| | AEPS6 | 0.911 | | | |
| BEIM | BEIM1 | 0.773 | 0.852 | 0.890 | 0.575 |
| | BEIM2 | 0.763 | | | |
| | BEIM3 | 0.777 | | | |
| | BEIM4 | 0.735 | | | |
| | BEIM5 | 0.758 | | | |
| | BEIM6 | 0.745 | | | |

| | | | | | |
|---|---|---|---|---|---|
| | CPFP1 | 0.885 | 0.954 | 0.962 | 0.783 |
| | CPFP2 | 0.898 | | | |
| | CPFP3 | 0.886 | | | |
| CPFP | CPFP4 | 0.881 | | | |
| | CPFP5 | 0.878 | | | |
| | CPFP6 | 0.871 | | | |
| | CPFP7 | 0.895 | | | |
| | PSDT1 | 0.902 | | | |
| PSDT | PSDT2 | 0.902 | | | |
| | PSDT3 | 0.896 | 0.940 | 0.954 | 0.806 |
| | PSDT4 | 0.897 | | | |
| | PSDT5 | 0.892 | | | |
| SCIP | SCIP1 | 0.809 | | | |
| | SCIP2 | 0.836 | | | |
| | SCIP3 | 0.803 | | | |
| | SCIP4 | 0.839 | 0.883 | 0.909 | 0.590 |
| | SCIP5 | 0.702 | | | |
| | SCIP6 | 0.673 | | | |
| | SCIP7 | 0.694 | | | |

**Table 2:** ***Discriminante Validity Heterotrait-Monotrait (HTMT) Ratio***

| | AEPS | BEIM | CPFP | PSDT | SCIP |
|---|---|---|---|---|---|
| **AEPS** | | | | | |
| **BEIM** | 0.540 | | | | |
| **CPFP** | 0.456 | 0.513 | | | |
| **PSDT** | 0.476 | 0.525 | 0.437 | | |
| **SCIP** | 0.555 | 0.676 | 0.587 | 0.564 | |

**Table 3:** ***Variance Inflation Factor (VIF)***

| Item | VIF | Item | VIF |
|---|---|---|---|
| AEPS1 | 3.675 | CPFP5 | 3.304 |
| AEPS2 | 3.809 | CPFP6 | 3.265 |
| AEPS3 | 3.381 | CPFP7 | 3.626 |
| AEPS4 | 3.869 | PSDT1 | 3.384 |
| AEPS5 | 3.458 | PSDT2 | 3.475 |
| AEPS6 | 4.188 | PSDT3 | 3.353 |
| BEIM1 | 3.131 | PSDT4 | 3.323 |
| BEIM2 | 2.848 | PSDT5 | 3.247 |
| BEIM3 | 3.152 | SCIP1 | 3.587 |
| BEIM4 | 2.868 | SCIP2 | 3.266 |

| | | | |
|---|---|---|---|
| BEIM5 | 2.934 | SCIP3 | 3.187 |
| BEIM6 | 2.844 | SCIP4 | 3.571 |
| CPFP1 | 3.399 | SCIP5 | 2.834 |
| CPFP2 | 3.853 | SCIP6 | 2.812 |
| CPFP3 | 3.518 | SCIP7 | 3.001 |
| CPFP4 | 3.414 | | |

**Hypotheses Testing**

**H1: Identity management that uses blockchain can positively and significantly impact the adoption of e-government payment system.**

The direction (> 0) of the path coefficient (= 0.210) is positive and meaningful because $t = 4.364$ and $p < .001$ are below 0.05. In addition, the statistical reliability of the finding is also enhanced since the 95% confidence interval (CI = [0.117, 0.303]) does not contain zero. This information confirms that the enhanced blockchain-based ID management practices will impact more positively the level of trust among the users and the likelihood of applying digital government payment solutions. This supports the argument that identity security procedures are key factors that affect the acceptance of digital financial systems by the user.

**H2: In cases where the payment processes are implemented in the form of smart contract, the implementation of the latter has a positive and strong effect on the use of e-government payment systems.**

The results *t*-value is 4.549 and a *p*-value of < .001 indicating the effect is significant and positive (i.e., 0.216). At this confidence interval (CI = [0.124, 0.308]), this relationship is statistically significant. This means that, in case the users could find the introduction of smart contract systems which have proven to be successful in the payment environment, then they would be more decisive to adopt e-government payment systems. This fact saves the importance of automating smart contracts as well as making them transparent and being reliable in enhancing the functionalities and appeal of that kind of system.

**H3: The use of e-government payment systems through the use of FinTech which involve cybersecurity practices is positively and significantly transformed.**

The relationship is also attested by the analytic results that have made statistically significant effect, path coefficient of 0.147, *t*-value of 3.226 and *p*-value of .001 and confidence interval of [0.059, 0.236]. This is the least of tested direct effects, but is important. The result indicates that a high-level cybersecurity of financial technology systems is one of the most important sources of trust that positively affects the use of e-government payment systems. Both protection, privacy and resistance to cyber threats will offer the required assurance and ensure that users feel more comfortable using the system.

It is established that BEIM, SCIP and CPFP and their relationships with AEPS are a positive and significant value, which as such reflects the locus of thought; that the three constructs are of paramount importance in defining how to use e-government payment platforms. The findings help justify the idea that conditions fostering technological tools namely identity management, smart contracts, and cybersecurity are essential catalysts to digital transformation in state financial services.

Advance Journal of Econometrics and Finance
Vol-4, Issue-2, 2026

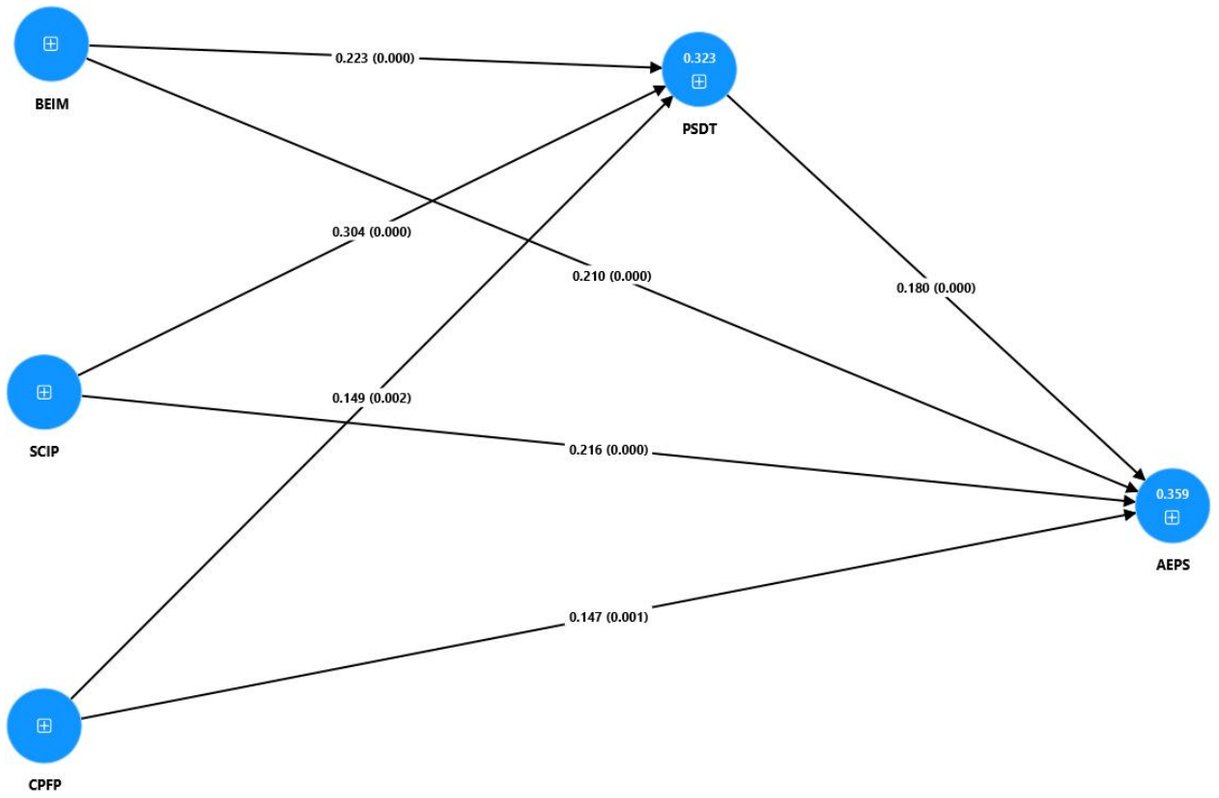


*Figure 4: Path Analysis of Model*

**Table 4:** *Summary of Direct Relationship Hypotheses Results (Bootstrapping Report)*

| Hypothesis | β Value | t-value | P - Value | C I (LL, UL) | Results |
|---|---|---|---|---|---|
| **H1**:BEIM→AEPS | 0.210 | 4.364 | 0.000 | (0.117, 0.303) | **Accepted** |
| **H2**:SCIP→ AEPS | 0.216 | 4.549 | 0.000 | (0.124, 0.308) | **Accepted** |
| **H3**:CPFP→AEPS | 0.147 | 3.226 | 0.001 | (0.059, 0.236) | **Accepted** |

*Note.* LL = Low Level, UL = Upper Level, CI = Confidence Interval.

**H 4: Perceived security of digital transaction in blockchain evoked identity management mediates between e-government payment system adoption and blockchain-enabled identity management.**

The mediation effect is significant (Res = 0.040, $t = 3.196$, $p = .001$) and the confidence interval (CI = [0.017, 0.068]) does not include the value of zero. However, there is a low mediation because the Variance Accounted For (VAF) is only 16.00%. This is to say that direct BEIM effect to AEPS (= 0.210) is still dominating even when the mediation of PSDT is taken. That is, BEIM directly affects AEPS with a small percentage of that impact on perceived security.

**H5: The implementation of smart contracts in payment and adoption of e-government payment systems have a mediating role played by perceived security of digital transactions.**

Both the direct and indirect effects of 0.055 are significant ($t = 3.322$, $p = .001$), and the reliability at that level is reasonable due to CI = [0.025, 0.089]. The VAF represents a partial-mediated 20.29%. It means that it will happen to have rather a great direct effect of (0.216) of SCIP on AEPS, however, a part of its effect has rather great indirect effect on PSDT. Thus, the adoption of smart contracts in improving the AEPS, especially when considering the customer perception of the security of the digital commerce, depends partially on how the customers perceive the security of the digital transactions.

**H6: Perceived security of digital transactions mediate the relationship between the digital security considerations in fintech platforms and the adoption of e-government payment platforms.**

The indirect impact = 0.027, $t = 2.541$, $p = .011$ and it is significant. This finding is also justified by the fact that the confidence interval (CI = [0.009, 0.049]) does not include 0, but the VAF (= 15.52%) is also weak mediation. This translates to the fact that where PSDT intermediates part of the relationship, CPFP is a direct cause of AEPS. The perception of security indeed increases the force of this pathway to a small degree but not the main channel.

The three hypotheses of mediation (H4–H6) have been confirmed that indicate that AEPS is an outcome of technological antecedents (BEIM, SCIP and CPFP) through the mediating role of Perceived Security of Digital Transactions (PSDT). SCIP is the strongest mediation with the PSDT application (20.29% VAF), which indicates the advantageous position of user trust regarding the safety of transactions that take place regarding smart contracts. However, it is more significant in relation to BEIM and CPFP because they rely on their immediate effect on adoption of AEPS even more. The complementarity of perceived digital security in facilitating adoption of e-government payment system in a technology-based acceptance is demonstrated by such findings.

**Table 5:** ***Mediation Type and Effect***

| Hypothesis | Indirect Effect (β) | t-value | P -Value | CI(LL, UL) | Direct Effect (β) | Total Effect (β) | VAF (%) | Mediation Result |
|---|---|---|---|---|---|---|---|---|
| **H4**:BEIM→ PSDT→AEPS | 0.040 | 3.196 | 0.001 | (0.017, 0.068) | 0.210 | 0.250 | 16.00% | Weak Mediation |
| **H5**:SCIP→ PSDT→AEPS | 0.055 | 3.322 | 0.001 | (0.025, 0.089) | 0.216 | 0.271 | 20.29% | Partial Mediation |
| **H6**:CPFP→ PSDT→AEPS | 0.027 | 2.541 | 0.011 | (0.09, 0.049) | 0.147 | 0.174 | 15.52% | Weak Mediation |

The values of $R^2$ indicate the proportion of the dependent variables variance, which is attributed to the individual predictor variables. Introduction of E-Government Payment Systems (AEPS) in this model shows that $R^2$ value equals 0.359 thereby revealing that nearly 35.9 percent of the overall variance of AEPS is explained by the independent constructs: BEIM, SCIP, CPFP, and PSDT. It is a being explanatory assertion, reasonable enough to apply in behavioral and social scientific study. Similarly, Perceived Security of Digital Transactions (PSDT) depends on BEIM, SCIP and CPFP to explain its own variance level, implying that 32.3% of its variance is achievable through BEIM, SCIP and CPFP. These values may be grouped as acceptable maximum variance account which according to Cohen (1988) values of $R^2$ above 0.26 are considered to have adequate levels of accountability with the captive of the structural model.

$Q^2$ statistics (check the model predictive relevance across the blindfolding process) are 0.287 and 0.257 using AEPS and PSDT, respectively. They are both positive thereby indicating that the model is predictively appropriate with respect to these important outputs. This has the implication that, this is not merely a model that explicates, but also has an ability in predicting the outcomes of AEPS and PSDT and within reasonable accuracy.

Results indicate that each predictor has small, but significant effects in effect size ($f^2$). BEIM with respect to AEPS has an effect size of 0.042 with a slightly higher effect size with PSDT of 0.046. CPFP corresponds to the level of equal, but insignificant impact on AEPS and PSDT (0.022). The standard effect numeral of SCIP on AEPS is also of the nature of a small effect, namely, 0.039 whereas its effect of 0.078 on PSDT lies on the goals of little and medium effect. A 0.02 to 0.15 represents small effects, but a pool of them in multivariate modelling may lead to very large volumes of the accounted variance (Cohen, 1988). All these findings suggest that no single construct has a dominant impact and that all technological elements—BEIM, SCIP, and CPFP—impactively bring about positive change in the perceptions of digital safety among users and adoption of government payment platforms. The model applies statistically adequate and useful evidence in drivers of the digital service adoption.

**Table 6:** ***Predictive Relevance, $R^2$, and Effect Size ($f^2$)***

| | AEPS | BEIM | CPFP | PSDT | SCIP |
|---|---|---|---|---|---|
| **AEPS** | | | | | |
| **BEIM** | 0.042 | | | 0.046 | |
| **CPFP** | 0.022 | | | 0.022 | |
| **PSDT** | 0.034 | | | | |
| **SCIP** | 0.039 | | | 0.078 | |
| **R-square** | 0.359 | | | 0.323 | |
| **Q-square** | 0.287 | | | 0.257 | |

Advance Journal of Econometrics and Finance
Vol-4, Issue-2, 2026


***Figure 5: $R^2$, $f^2$, and $Q^2$ Charts***

**Discussion**

This paper has indicated the significance of safe and trustable technology in adoption of e-government payment systems (AEPS). One of the technological constructs that was tested had significant effects on AEPS, and it was outstanding in identity management of blockchain-based identity management (BEIM). It can be explained by the growing body of evidence indicating that decentralized identity models have the potential to advance transparency and data integrity that, in turn, boost the degree of the public trust elected towards online platforms (Alketbi et al., 2018; Zheng et al., 2018). One can also find this represented in recent developments. A good case in point is the RealDID project in China, which integrates identifiers based on blockchains in national digital identity systems, which marks the viability of BEIM in increasing the provision of services and privacy levels (Wikipedia, 2025). In addition to that, governments in more than 130 countries actively pursue or also use blockchain as a digital identity, which justifies its importance in the provision of governmental services (Yellow, 2025).

The payments component, the implementation of Smart contract made payment (SCIP) was the most potent component of the model. It aligns with the recent empirical studies of smart contracts significantly reducing the friction in the financial activities by automating household trust and compliance (Christidis & Devetsikiotis, 2016; Rejeb et al., 2022). There is a growing acceptance of smart contract system in the industry and it is approximated that it will experience a colossal expansion in the coming 10 years (Precedence Research, 2025). Such perception of automation and openness builds more trust in users toward the e-government payment systems. Besides, the implementation of verification based on AI and the need to use smart contacts has also attracted some research in order to enhance the efficiency and empowerment of the users in the systems (Xavier et al., 2024).

One more study confirms the importance of cybersecurity protocols on fintech platforms (CPFP) and, however, with a comparatively low influence compared to BEIM and SCIP. The results are consistent with emerging body of evidence to show that, despite the significance of cybersecurity as an integral part of trust, it is perceived as essential infrastructure instead of a driver of adoption (Safa et al., 2016; Akinyemi & Adewole, 2020). As such threats in digital form become increasingly sophisticated, and governments become the biggest target of such threats, cybersecurity becomes a pivotal component of reliability or continuity (McKinsey & Company, 2024).

The mediating role of perceived security of digital transactions (PSDT) also offer material suggestions about the analysis that users give on the security of their transactions. The three technological antecedents thus BEIM, SCIP and CPFP all influenced AEPS albeit to certain extent through PSDT. The mediated effect on SCIP was the most prominent therefore affirming the role of user-perceived security in mediating an outcome of adoption. It is also aligned with other technology acceptance (TAM) models and related models, perceived trust and concept of security elements are central to the user adoption (Venkatesh et al., 2003).

The predictive perspective shows that the model has a moderate power of explanation and a great predictive significance that does not fail to forecast either AEPS or PSDT. The results are in line with the existing literature that proposes inclusive models of the digital transformation, i.e., synthesis of the infrastructural proficiency with user-based constructs, including perceived security, and transparency (Rejeb et al., 2023).

This implication of the study, however, can be implied to be seen in the perspective of new complexities. Even though the smart contracts are treated as a revolution, according to legal experts, it faces problems in enforcement and error and uncertainty in regulations (Arif et al., 2025; The Fintech Times, 2025). Moreover, the difference in user literacy and digital sophisticability, as well as in state confidence, can even out the regional adoption patterns - a point worth taking into consideration in case of a comparison in the future.

Comprehensively, the current study injects empirical support on the argument that technological innovation ought to be matched by perceived security to the users to achieve the potential in online payment systems applied by all government systems. It can also be aided with blockchain identities, smart contracts and cybersecurity, but the combination of these concepts together with the perception of users will compel them to implement it.

**Theoretical Implications**

The output of this work helps to form the theoretical foundation of the study of technology adoption regarding the public digital services (that is, e-government payment systems) in a variety of issues of importance.

The first, it extends Technology Acceptance Model (TAM) to include more advanced technological constructs absent in traditional models, i.e., Blockchain-Enabled Identity Management (BEIM), Smart Contract Implementation for Payments (SCIP), and Cybersecurity Protocols in FinTech Platforms (CPFP). This fusion of the two attributes causes the study to become more current and situation-dependent in terms of understanding adoption behavior in digital financial systems.

Second, the research conclusions are applied and substantiated in a comprehensive manner, indicating that besides perception of ease of use and usefulness, the perceived security (PSDT) is a partial mediator in the process of adoption. This is an important twist in the contemporary models: even in highly developed systems users should feel secure in using them, which underpins the importance of entrenching constructs of trust on the existing theories.

Third, the study supplies empirical evidence on the premise that the technological infrastructures and psychological perception rely on each other. Though both BEIM and SCIP can have a direct influence, through the partial mediation of PSDT it is clear the perceived security is not merely a by-product of system quality, but rather a critical process whereby pre-determining the outcome of behavior. This is contributing to the emerging theoretical support that perceptions of user trust should be considered in disruptive technology measuring models.

Finally, by application to the e-government services, the paper shall contribute to the growing literature on the matter of innovation in the public sector, which could implement models rather differently than in non-governmental or commercial environment. The given theoretical implementation can become the way to address the existing gap between the literature about digital government and technological adoption research.

**Practical Implications**

In regard to policy and implementation, this study gives as among its working recommendation to the governments and the designers of the digital platforms as much as it does to the technology planners among the masses.

To begin with, the sheer force of the identity management aimed at utilizing the blockchain, or rather BEIM, makes one conclude that the governments should direct their attention to developing and deploying the safe and decentralized identity infrastructures. This data integrity and fighting fraud not only, but also builds user confidence that pillar to service acceptance.

Second, Smart Contract Implementation of Payments (SCIP) is an essential attribute to consider that entails the fact that automating payments and transparency are the keys to enhancing citizen confidence. Governments in situations where accountability, efficiency and transparency are the main issues should consider investing in smart contract-based smart systems in the execution of the government financial transactions.

Third, with a rather minimal impact of Cybersecurity Protocols (CPFP), the findings justify its facilitative role. To enhance the image regarding the stability and credibility of the system, the agencies ought to make sure that they possess stringent cybersecurity frameworks and spread the safety provisions to its consumers.

Fourth, the communication strategies toward users should be targeted as Perceived Security of Digital Transactions (PSDT) is a mediator variable. Besides the development of secure technology, the government services must also emphasize on security education, interface openness and awareness that will enhance the security of user information and that of their transactions.

Finally, due to the mid-predictive nature of the model, the governments are advised to explore the idea of co-layered digital strategies that ensure that the increment of back-end technology, front-end user experience, and perceived security are strengthened and consistent in response. Such a hybrid solution is more likely to be adopted, more likely to lead to the introduction of more satisfaction among the citizens, and thus more successful in transforming governmental services in a digital way.

**Conclusion**

In this paper, the technological and perceptual drivers that influence the adoption of the e-government payment system were studied with reference to three main constructs, namely: Blockchain-Enabled Identity Management (BEIM), Smart Contract Implementation with Payments (SCIP), and Cybersecurity Protocols in FinTech Platforms (CPFP), where Perceived Security of Digital Transactions (PSDT) was a mediating variable.

The findings affirm the fact that the three technological constructs have the positive and significant effects on adoption and the SCIP has the most significant effect on adoption than BEIM and CPFP. The given findings indicate the importance not only of better development of digital infrastructure, but also of a clear vision that these technologies will be considered safe and reliable by the users. The mediating role of PSDT albeit to a small level and with a dynamic extent further confirms the reality that the perception of security is centrally placed in the determination of how the users act, particularly when communicating within an electronic environment whose most influential features are trust and transparency.

The theoretical contribution of the study lies in the use of traditional models concerning the use of technology by incorporating new emerging digital technologies besides constructs that incorporate trust. It also provides reasonable recommendations to governments and developers of digital platforms, as well as caution on extensive approaches that include secure technical architecture in combination with communicative and user-centric approaches.

To conclude, to successfully introduce e-government payment systems, it is necessary to give attention not only to the advantages of such a technological option as blockchain-based identity and smart contracts but also to the aspect of how safe the interactions with users are perceived to be. The difference between the technical potential and its perception by the user will be decisive to the processes of mass and long-term adoption of digital public services.

**Restrictions and Future Work**

Even though this study provides valuable information regarding both the technological and perceptual variables with regard to the implementation of e-government payment systems, several limitations are to be mentioned. One of the limitations is that it used cross-sectional research design which reflects the responses at a point in time. This restricts the ability to create causality or even the direction (topos) in which perceptions and adoption behaviors are going to vary over time. Future studies should employ the longitudinal or experimental research in order to get a better understanding of how user engagement with new technologies can be dynamic.

The other weakness relates to the contextual area coverage of a sample. It is possible that its outcomes are connected to the characteristics of a certain geographic region, society, or the level of the digital infrastructure development. Because societies vary in user trust, regulatory environment and digital literacy, this reduces the externalization of the results. The next research should also concentrate on validating the relevance of this model on different areas or conduct a comparative research to establish how the local factors impact on the adoption patterns.

Besides, the study was examining a certain scope of constructs including Blockchain-Enabled Identity Management (BEIM), Smart Contract Implementation (Payments) (SCIP), Cybersecurity Protocols in FinTech Platforms (CPFP) and Perceived Security of Digital Transactions (PSDT). These as well as other variables such as digital literacy, perceived risk, and government transparency or user resistance to technology were not mentioned although they are just as relevant. It is possible to take these factors into account in subsequent investigations in which more vivid models of users in online governmental circumstances are to be developed.

Unlike in the case of perceived security which underwent testing as a mediating variable, it can be presumed that other mediating variables/moderators can also be considered. Indicatively, the government-associated institutions, the ease of use, or the ease of use of digital interfaces attracts influence on the adoption outcomes as well. By adding such constructs it can reasonably be expected that it can give a better interpretation of the user perceptions and how they use e-government services.

Finally, as technology rapidly accelerates, new forms of digital infrastructure are beginning to remodulatively alter service provision in the state sector, such as decentralized autonomous organizations (DAOs), artificial intelligence-based service platforms, or quantum-resistant systems of payment. In this respect future research has to respond to such changes by frequently updating the theoretical frameworks and empirical guide models to ensure that they are not left behind in the dynamic aspects of emerging technology.

**References**

Abubakar, A. K., et al. (2025). The role of the Internet of Things (IoT) in achieving the United Nations (UN) Sustainable Development Goals (SDGs) A systematic review. *ACM Computing Surveys*.

AlBliwi, S. A., et al. (2025). Service quality and consumer behavior in Saudi Arabia: Examining transactions and technological integration within the Vision 2030 framework. *European Journal of Sustainable Development*, *14*(2), 451.

Al-Hajri, A., et al. (2024). A systematic literature review of the digital transformation in the Arabian Gulf's oil and gas sector. *Sustainability*, *16*(15), 6601.

Alhejaili, M. O. M. (2024). Securing the Kingdom's e-commerce frontier: Evaluation of Saudi Arabia's cybersecurity legal frameworks. *Journal of Governance and Regulation*.

Ali, B., et al. (2025). Antecedents of post-adoption continuous usage intention of e-wallet (Easy Paisa) in Pakistan: A UTAUT perspective. *Social Science Review Archives*, *3*(3), 882–907.

Ali, M. A., & Salih, S. M. (2025). Impact of Application Programming Interfaces (APIs) economy on digital economics in Saudi Arabia. *Sustainability*, *17*(9), 4104.

Almutairi, I. L., et al. (2022). Managing entrepreneurship during the COVID-19 pandemic crisis in the State of Kuwait: The relevance of technology and innovation. *International Journal of Early Childhood Special Education*, *14*(3).

Aloulou, M., et al. (2024). Does FinTech adoption increase the diffusion rate of digital financial inclusion? A study of the banking industry sector. *Journal of Financial Reporting and Accounting*, *22*(2), 289–307.

Alsakhnini, M., & Almoaiad, Y. (2024). A review of applications of blockchain technology in the Middle East. *Kurdish Studies*, *12*(1), 103–130.

Alshaikh, M., et al. (2025). The impact of cybersecurity through knowledge sharing practices: Limitations, analysis of current trends and future research directions. *International Journal of Advanced Computer Science & Applications*, *16*(3).

Altwijry, O., et al. (2023). Financial technology and Islamic insurance: The Saudi context. *Scientific Journal of King Faisal University, Humanities & Management Sciences*, *24*(2).

Alwadain, A., et al. (2024). From theory to practice: An integrated TTF-UTAUT study on electric vehicle adoption behavior. *PLOS ONE*, *19*(3), e0297890.

Baldi, G., & Botti, A. (2024). An alternative view on smart cities: Can small towns become smart? In *Smart cities* (pp. 202–219). Routledge.

Baroudi, S., & Benghida, S. (2022). Blockchain in Dubai: Toward a sustainable digital future. In *Contemporary research in accounting and finance: Case studies from the MENA region* (pp. 253–271). Springer.

Chachi, A., et al. (2024). *Digital transformation of payment systems in OIC member countries*.

Chen, J. (2023). Design of e-government platform based on cloud computing in the era of big data. *International Conference on Mathematics, Modeling, and Computer Science (MMCS2022)*. SPIE.

Das, D. K. (2025). Digital technology and AI for smart sustainable cities in the global south: A critical review of literature and case studies. *Urban Science*, *9*(3), 72.

Deek, A. Y. A. (2024). *Palestine, the real startup nation: A vision for the next generation role model for technological innovation and economic transformation* (Doctoral dissertation, AAUP).

Douaioui, K., & Benmoussa, O. (2024). Insights into industrial efficiency: An empirical study of blockchain technology. *Big Data and Cognitive Computing*, *8*(6), 62.

Douffi, G., & Dahman, N. (2025). Requirements for activating digital finance in Algeria in lights of the Saudi experience. *Mila Journal for Research and Studies*, (111), 280–299.

ESCAP, U. (2022). *Frontier ICTs for sustainable development for digital leaders: Submodule C: Internet of Things*.

Farhah, M. F. A. (2022). The blockchain: The next technological revolution in the world of the economy. *Journal of Economic, Administrative and Legal Sciences*, (615), 119–140.

Garg, M., & Kumar, P. (2024). Harnessing digital technologies for triple bottom line sustainability in the banking industry: A bibliometric review. *Future Business Journal*, *10*(1), 62.

Guo, Y. (2023). How does culture influence Chinese people's views and actions on e-government websites? A study on citizens' continuous use of e-government websites based on cultural model. *Proceedings of the 24th Annual International Conference on Digital Government Research*.

Harunoğullari, E. (2025). An analysis of disruptive technologies in Muslim societies: Economic, financial, and ethical implications. In *Disruptive technologies and Muslim societies: From AI and education to food and fintech* (pp. 389–416). World Scientific.

Huseynov, A., et al. (2025). Challenges and opportunities of digital economy development: Case of Azerbaijan. *Problems and Perspectives in Management*, *23*(2), 265.

Ionașcu, A. E., et al. (2023). Unraveling digital transformation in banking: Evidence from Romania. *Systems*, *11*(11), 534.

Jena, R. (2023). Factors impacting senior citizens' adoption of e-banking post COVID-19 pandemic: An empirical study from India. *Journal of Risk and Financial Management*, *16*(9), 380.

Khan, A. I., et al. (2022). Integrating blockchain technology into healthcare through an intelligent computing technique. *Computers, Materials & Continua*, *70*(2), 2835–2860.

Khan, M. Z. (2022). *Role of central bank digital currency (CBDC) for financial inclusion in Organization of Islamic Cooperation (OIC) countries* (Doctoral dissertation, Hamad Bin Khalifa University, Qatar).

Khang, A. (2025). *Shaping cutting-edge technologies and applications for digital banking and financial services*. Productivity Press.

Kumar, A., et al. (2022). Smart cities: A step toward sustainable development. In *Smart cities* (pp. 1–43). CRC Press.

Makki, A., & Alqahtani, A. (2022). Modeling the enablers to FinTech innovation in Saudi Arabia: A hybrid approach using ISM and ANP. *Systems*, *10*, 181.

Mohamed, S. K., et al. (2023). Blockchain technology adoption for improved environmental supply chain performance: The mediation effect of supply chain resilience, customer integration, and green customer information sharing. *Sustainability*, *15*(10), 7909.

Mostenska, T. G., et al. (2025). *Innovative approaches to the use of artificial intelligence in countering disinformation: EU experience and prospects for Ukraine*. Publishing House "Baltija Publishing".

Mustafa, M. H., et al. (2025). The importance of empowering the smart city in Iraq: A case study of Baghdad municipalities. *International Journal of Sustainable Development & Planning*, *20*(3).

Nam, J., et al. (2025). Amusement as key motivation: Informing client needs in CMC technologies for enhanced collaboration. *IJIKM*, *20*.

Negm, E. M. (2024). Consumers' acceptance intentions regarding e-payments: A focus on the extended unified theory of acceptance and use of technology (UTAUT2). *Management & Sustainability: An Arab Review*, *3*(3), 340–360.

Nguyen, N.-T. T., et al. (2024). The future of non-contact commerce: The role of voice payments. *Journal of Financial Services Marketing*, *29*(4), 1260–1278.

Noreen, U., et al. (2023). Banking 4.0: Artificial intelligence (AI) in banking industry & consumer's perspective. *Sustainability*, *15*(4), 3682.

Oyekola, O. A. (2023). *How organizational agility can contribute to effective digital transformation in international financial institutions* (Doctoral dissertation, University of Maryland).

Piaggesi, D., et al. (2022). *Cases on applying knowledge economy principles for economic growth in developing nations*. IGI Global.

Quamar, M. M., et al. (2023). Bahrain. In *Persian Gulf 2023: India's relations with the region* (pp. 41–80). Springer.

Rashid, E. M. (2023). The digital reality of the United Arab Emirates in light of technological and informational developments. *Economic and Administrative Studies Journal*, *2*(2), 1–15.

Rey, W. P., & Rey, K. W. J. D. (2024). Optimizing WeBarangay: A comprehensive performance and security audit. *2024 3rd International Conference on Computer Technologies (ICCTech)*. IEEE.

Roslan, M. A. A., et al. (2024). Understanding technology acceptance and use in social media platforms: A systematic literature review and the development of research framework. *Journal of Social Computing*, *5*(3), 261–291.

Saim, M., & Traore, M. (2025). The future of public financial management systems: Embracing digital transformation and smart government services. *Revue Algerienne De Finances Publiques*, *15*(1), 63–76.

Sauvant, K. P., et al. (2022). *An inventory of concrete measures to facilitate the flow of sustainable FDI: What? Why? How?*

Shahid, M. (2025). *Tokenized property ownership: Legal recognition and compliance framework*. Available at SSRN 5386108.

Susanty, A., et al. (2025). Factors influencing the intention of textile and garment SMEs to adopt digital technologies and its impact on performance. *Scientific Reports*, *15*(1), 20807.

Tian, Z., et al. (2024). Drivers and influencers of blockchain and cloud-based business sustainability accounting in China: Enhancing practices and promoting adoption. *PLOS ONE*, *19*(1), e0295802.

Tiika, B. J., et al. (2024). Evaluating e-government development among African Union member states: An analysis of the impact of e-government on public administration and governance in Ghana. *Sustainability*, *16*(3), 1333.

Wang, T., et al. (2022). *G20 toolkit for measuring digital skills and digital literacy: A compilation of reports*.

Xin, C. S. M., et al. (2023). *Malaysian expectation towards digital banking*.

Youssef, N. (2025). The impact of financial technology innovation on bank's financial performance: Evidence from Egypt. *Journal of Commercial Research*, *3*, 60–97.

Zayani, M., & Khalil, J. F. (2024). *The digital double bind: Change and stasis in the Middle East*. Oxford University Press.