Artificial Intelligence (AI) and Blockchain-based Online Payments in the Global World

Ahlam Alhalafi [1] and Prakash Veeraraghavan [1], Dalal Hanna [2]
Ahlam.Alhalafi@hotmail.com P.Veera@latrobe.edu.au D.Hanna@latrobe.edu.au n.alhalafi@hotmail.com
La Trobe University, Computer Science & Information Technology Department, Australia

Abstract
Payment systems are evolving, and this study examines how blockchain and AI improve online transactional security and service quality. The study examines micro and macro payment systems, compares online, and offline methods all over the world. The study also examines how blockchain and AI affect payment system security, privacy, and efficiency globally and rapidly digitizing economy. Digital payment methods are growing all over the world with high literacy and digital engagement, but they face challenges. The research highlights cybersecurity threats and the need to balance user convenience and security. It suggests blockchain and AI improve online payment services, supporting the policies for different countries. In this extensive research survey, we compare and evaluate the strengths and weaknesses of various payment systems, their practicality, and their robustness. This study *also* examines how technological innovations and payment systems interact to reveal how blockchain and AI could transform the financial sector. It seeks to understand how technology-enhancing service quality can boost customer satisfaction and financial stability in the digital age. The findings should help policymakers, financial institutions, and technology developers optimize online payment systems for a more secure and efficient digital economy.

Keywords:
AI, blockchain, online payments, digitalized economy, sustainable development, global world

1. Introduction

The diversification and evolution of payment systems in the dynamic realm of digital commerce bears witness to the progress of technology and its assimilation into the financial industry. Payment systems cover the entire range of financial transactions, from modest, routine purchases to large, important financial exchanges. They are generally divided into two categories: micropayments and macro-payments. Access to digital goods and services depends on micropayments, which are designed for small digital transactions and have the potential to drastically transform digital commerce by providing new revenue streams outside of traditional advertising models. The efficiency and security of these transactions have increased thanks to innovations like decentralized anonymous micropayment schemes and duplex micropayment channels. In addition, macro payments are more complex and involve larger amounts of money, which means they require strong security and complicated regulatory compliance, particularly in industries like real estate and luxury goods. Technology is becoming more and more integrated into payment systems; this is evident in the contrast between online and offline methods, which offers speed and convenience but also raises security, privacy, and user experience concerns.

In tackling these issues, the introduction of blockchain technology and artificial intelligence (AI) into online payment systems represents a major advancement. With its decentralized and unchangeable ledger system, blockchain technology has improved data integrity, decreased fraud, and boosted security—all of which are especially important for large-scale micro-payments. Simultaneously, AI improves decision-making and customer service, maximizing e-commerce and streamlining transactions. The utilization of these technologies is especially relevant when considering countries with a high level of education, a high rate of internet and mobile penetration, and a willingness to accept digital banking. Threats to cybersecurity and the need to strike a balance between user convenience and strict security measures are still issues, though. It is imperative to understand and capitalize on the correlation between service quality and technology adoption in online payments, particularly in light of MENA region's swift digital transformation. In order to support sustainable financial performance, this study intends to investigate how the combination of blockchain technology and AI improve the quality of online payment services. The goal of the research into these dynamics is to shed light on the possible advantages for the financial industry, including improved customer satisfaction and financial stability in an increasingly digital environment.

2. Literature review

2.1 Challenges of online payments

The development of online payment methods has revolutionized the world of finance by providing unmatched efficiency and convenience. However, there are

Manuscript received March 5, 2024
Manuscript revised March 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.3.1

drawbacks to this progress as well. These challenges are diverse, varying depending on the area and technology. Making sure there is strong security and privacy when making payments online is one of the main challenges. Although the introduction of blockchain technologies has revolutionized the security aspect of online transactions, worries about their susceptibility to sophisticated cyber threats persist, as noted by Ducas and Wilner (2017) and Chiesa et al. (2017). According to Al Zoubi (2023), who addresses the cyber security issues facing Saudi Arabian financial services, this is particularly relevant and reflects a global concern in the fintech industry. While integrating biometric authentication systems offers a promising way to improve security, there are drawbacks, including privacy issues and potential technological failures (Ogbanufe & Kim, 2018; Talib & Salman, 2022).

Adopting and integrating these cutting-edge technologies into the current financial infrastructures presents a considerable challenge. The research conducted by De Luna et al. (2019) and Karim et al. (2021) highlights the disparities in technology adoption levels among various geographical areas, which can be attributed to various factors, including consumer confidence, technological proficiency, and infrastructure preparedness. This is made more difficult by the fintech industry's rapid evolution of innovations, as discussed by Agarwal and Zhang (2020) and Harris and Waggoner (2019), which calls for constant development and adaptation. According to Huang et al. (2021), the COVID-19 pandemic has significantly affected how online payments are shaped, hastening the transition to digital transactions. The unexpected increase in online financial activity has highlighted the need for reliable and scalable payment systems. However, as Jiang et al. (2015) and Oo (2019) point out, the pandemic also exposed the digital divide, which puts people at a disadvantage if they have limited access to digital infrastructure.

As examined by An et al. (2021) and Sandner et al. (2020), the incorporation of cutting-edge technologies like blockchain and artificial intelligence (AI) in online payment systems offers both opportunities and challenges. As noted by Mavroeidis et al. (2018) and Muheidat et al. (2022), adopting these technologies presents concerns about technological interoperability, regulatory compliance, and the requirement for specialized skills, even though they offer increased efficiency, transparency, and security. Regulators, financial institutions, and technology providers must work together to navigate these challenges effectively.

2.2 Classification of Payment System

The landscape of payment systems constantly changes as commerce and developing digital technologies converge. Different systems have evolved to handle everything from tiny financial exchanges to massive ones. The following discussion focuses on micropayments, macro payments, and the comparison of offline and online payment systems to better understand these classifications.

2.3 Micro Payments

Designed for quick financial transactions, micropayments primarily support the purchase of digital goods and services. According to Rußell et al. (2020), micropayments are essential for low-priced digital goods transactions. They act as a portal to abundant digital resources, from premium digital content to features unique to specific apps. While this is happening, Clarke & Pucihar (2019) highlighted how micropayments are reshaping digital commerce and giving businesses new ways to monetize outside conventional ad-based models. Decker & Wattenhofer (2015) found that Duplex micropayment channels significantly enhance Bitcoin's scalability and speed for real-time transactions. By using hashed time lock contracts, these channels ensure secure, non-reversible transfers with minimal fees. This innovation positions Bitcoin for instant micropayments, akin to the speed of internet messaging.

Chiesa et al. (2017) developed Decentralized anonymous micropayment (DAM) that schemes offer a method for conducting offline probabilistic payments privately on ledgers. Key to this process is the fractional message transfer (FMT) that allows for probabilistic message transmission. However, while double spending cannot be entirely prevented, its potential utility is constrained by advanced deposits that are forfeited upon detecting cheating. In addition, Puspadini, Yudhapramesti & Bakry (2023) described that the primary motive for audiences accessing DailySocial.id, a micro-paid news portal, is navigability, emphasizing the freedom to explore information. Entertainment and fun are the main gratifications sought by users. A significant 76% of the audience is inclined to purchase micro-paid articles, with access frequency and duration being crucial factors. Heilman, Baldimtsi & Goldberg (2016) introduced an eCash-inspired method to boost anonymity in on and off-blockchain Bitcoin transactions. Our techniques ensure fair-exchange resistance to forgery, double spending, DoS, and Sybil attacks. However, achieving full anonymity against a malicious intermediary in off-blockchain schemes remains an open challenge.

2.3.1 Benefits and Limitations of Micro Payments

Micro Payments are appealing because they can offer a seamless customer experience, especially for small amounts. They are valuable in lowering consumer transactional friction, according to Liébana-Cabanillas et al. 2022). Some obstacles loom large. High transaction fees, which frequently threaten to surpass the principal

transaction amount, have become a growing source of industry concern, according to Kumar et al. (2021), raising questions about the viability of such systems. Micropayment systems have proven to have a lot of potential and efficiency, especially those built on blockchain technology and cryptocurrencies like Bitcoin. However, their widespread use and seamless operation are subject to several restrictions. For example, Decker and Wattenhofer (2015) discussed the difficulties of scaling Bitcoin and emphasized the demand for effective payment networks. Although effective, their solution—the duplex micropayment channels—involves setup and dispute resolution difficulties. Furthermore, Heilman, Baldimtsi, and Goldberg (2016) hinted at the issues with transaction anonymity, highlighting the distinction between on-chain and off-chain Bitcoin transactions to highlight how difficult it is to maintain anonymity in some transaction scenarios.

Decentralized anonymous micropayments have a lot of potential. However, Chiesa et al. (2017) also noted that there are still issues with achieving total anonymity, mainly when dealing with a bad intermediary in off-blockchain schemes. While Puspadini, Yudhapramesti, and Bakry (2023) found a lot of interest in adopting micropayments in the media sector, they still need to address the more general problems of consumer consumption patterns and behavioral tendencies in various populations. This creates a knowledge gap regarding the potential acceptance of micropayments in various cultural or regional contexts. To overcome these obstacles, ongoing research, and technological advancements are required to make micropayments more effective, anonymous, and universally applicable.

2.4 Macro Payments

The need to enable safe, effective, and easily accessible financial transactions has fueled continuous innovation and development throughout online payments, both at the macro and micro levels. At first, online payment systems were primarily designed to handle macro-transactions, but more significant financial transactions are commonly observed in business-to-business (B2B) settings. These systems were developed using credit card networks and electronic funds transfer (EFT) over conventional banking infrastructures. Micro-payment platforms were introduced due to the need to create more flexible payment options due to the rise of e-commerce. These platforms were created with an emphasis on usability, low transaction costs, and scalability in order to manage smaller transactions, usually in business-to-consumer (B2C) and consumer-to-consumer (C2C) scenarios, as covered in the works of Decker and Wattenhofer (2015) and Chiesa et al. (2017). As Kumar et al. (2021) and De Luna et al. (2019) discussed, micro-payments were expanded with the introduction of digital wallets and mobile payment technologies, enabling smooth and quick transactions, even for small amounts.

The evolution of online payment systems has entered a new era by integrating (1) blockchain technology and (2) AI. According to Mavroeidis et al. (2018) and An et al. (2021), blockchain technology provides a decentralized, secure ledger system, significantly improving the security and transparency of online transactions. This technology plays a critical role in safeguarding transaction record integrity and preventing fraud. However, as Harris and Waggoner (2019) and Gulati et al. (2020) discussed, AI enhances the intelligence and flexibility of payment systems. AI algorithms enhance online payment systems' effectiveness and user experience by detecting fraud, risk assessment, and personalized services. According to Sandner et al. (2020) and Li (2020), the combination of blockchain technology and AI is particularly revolutionary, providing solutions that are not only intelligent and adaptable to changing market conditions but also secure and decentralized. These technologies are essential to the current state of online payments because they guarantee security, efficiency, and scalability while meeting micro and macro transactional needs.

In sharp contrast, macro payments allow for sizable financial transactions, also known as sizeable purchases. Given the sizeable sums involved, Ducas & Wilner (2017) called attention to the necessity of security in macro payments. These transactions involve more than just the money transfer, mainly when they involve industries like real estate or luxury goods. They involve intricate contractual stipulations, recurring payments, and complex regulatory compliances. The stock-flow consistent (SFC) model, rooted in 1970s research, has gained traction in macroeconomics, particularly after its successful prediction of the 2007-9 Great Recession (Nikiforos & Zezza, 2018). The approach offers insights into financialization, income distribution, and the dynamics of macro payments. Furthermore, it is integrated into agent-based microeconomic models and forms the basis for ecological macroeconomics research.

Sinha & Singh (2023) assessed factors influencing Indian merchants' intentions to use mobile payment services (MPS). Among six factors studied, the perceived experience was the most influential, followed by word-of-mouth learning. Additionally, perceived experience mediated and moderated the relationship between word-of-mouth learning and intention to use MPS. These insights are valuable for financial entities aiming to understand and boost MPS adoption among merchants. Therefore, macro payments are handled online via different channels and platforms.

2.5 Online versus Offline Payment Methods

Payment systems are split into offline and online mechanisms at a basic level. De Luna et al. (2019) noted a continued reliance on traditional payment methods like cash and checks, particularly among older people and in areas with spotty internet access. On the other hand, online payment systems—that include e-wallets, bank transfers, and card payments—speak the language of contemporary convenience. Gomber, Koch & Siering (2017) emphasized how closely these systems are related to the e-commerce boom and a rapidly digitizing global economy.

The global fintech industry prioritizes real-time security in online payments, emphasizing the need for robust, adaptive, and proactive security. Advanced security protocols are needed as digital transactions become more common and vulnerable to cyberattacks. Ducas and Wilner (2017) and Chiesa et al. (2017) show that blockchain technology can reduce fraud and data breaches using decentralized and immutable ledgers. According to Ogbanufe and Kim (2018) and Talib and Salman (2022), biometric authentication adds security by using unique personal identifiers to prevent unauthorized access and transactional fraud. According to Harris and Waggoner (2019) and Sandner et al. (2020), AI in online payment security uses machine-learning algorithms to detect and stop potential security breaches in real-time. According to Mavroeidis et al. (2018) and Giudici (2018), the rapid advancement of quantum computing poses new challenges that could make some cryptographic methods obsolete, prompting the evolution and adaptation of security strategy. This dynamic landscape emphasizes the need for real-time security research and development to protect online payment systems worldwide.

The clear trend towards online payment methods cannot be disputed. The rapid digitization of services, Fintech innovations, and growing user comfort with online platforms were some factors that Agarwal & Zhang (2020) identified as driving this transition. The broader repercussions are significant. Beyond mere convenience, these systems, according to Zhou & Clark (2023), are poised to redraw the lines dividing international trade, resulting in a more interconnected, immediate, and borderless transactional ecosystem.

The potential for innovation increases as the payment universe's horizon does. Shortly, where offline and online payment methods may not stay distinct but may merge, creating hybrid systems, Huang et al. (2021) painted a vivid picture. Such a development would combine the best features of both worlds and provide customers with various options catered to transactional requirements. The complex world of payment systems is proof of human ingenuity and the unrelenting advance of technology. The financial tapestry is rich and diverse, ranging from micro to macro systems and the ongoing dance between offline and online methods. The ongoing challenge will be to improve these systems so that they are supported by solid security, transparency, and inclusivity principles while also elevating convenience.

3. Online Payment Systems:Privacy, Security, and Anonymity

3.1 Privacy and Anonymity

The digital economy now relies heavily on online payment systems because they promise convenience and speedy transactions. The guarantee of user privacy is one of the essential tenets supporting the success of these platforms. Regarding online payments, privacy refers to protecting personal data and securing it from unauthorized access (Oo, 2019). However, complete privacy assurance does not ensure anonymity. Online anonymity refers to the capacity to make payments without disclosing one's identity. Although there are some difficulties due to the traceability of blockchain, cryptocurrencies like Bitcoin offer a layer of anonymity in transactions because they do not directly link transactions to personal details (Berentsen, 2019).

Recent literature emphasizes the importance of online payment privacy and anonymity. Regner and Riener (2017) emphasize the importance of privacy, especially in online transactions, where lifting anonymity can cause consumer apprehension and revenue loss for businesses. Balgobin et al. (2016) examine how financial privacy affects online shopping. Their findings indicate that users prefer anonymous payment methods, emphasizing the importance of privacy in e-commerce. Schomakers et al. (2020) examine users' preferences for privacy-preserving data markets and find that consumers are increasingly concerned about their data and its use in online transactions.

Anonymity in online payments protects users' identities and financial information. Khalilov and Levi (2018) survey anonymity in bitcoin-like digital cash systems, showing how cryptocurrencies address privacy concerns. Goldfeder et al. (2017) discuss the privacy risks of web payments with cryptocurrencies, especially when cookies and blockchain technology interact. These studies show that cryptocurrencies increase anonymity but also raise privacy concerns.

Perfect anonymity in online payments is challenging. Garman, Green, and Miers (2017) discuss accountable privacy in decentralized anonymous payments and the need to balance user anonymity and legal accountability. This balance is essential to prevent money laundering and fraud, which thrive anonymously. Further, Rajendran et al. (2017)

discuss the implementation challenges of secure and privacy-preserving digital payment systems that comply with regulations and protect user data. These studies show how difficult it is to protect user privacy and anonymity in online payments, highlighting the need for innovative solutions that balance security and legal compliance. Over time, this field has realised the importance of privacy in online financial transactions and the need for robust, transparent, and user-friendly solutions.

3.2 Identity Verification Methods

In digital payments, it is crucial to guarantee that users' identities are confirmed. Because of cyberattacks, password-based authentication, which has historically been the most common, is becoming more vulnerable (Jiang et al., 2015). Technology advancements have fueled the growth of biometric authentication methods like Face ID and fingerprints. These techniques are thought to be more secure against breaches because they are based on the distinctive biological traits of each individual (Talib & Salman, 2022). Using two-point or multi-point authentication also adds another layer of security to the system. Users go through several levels of verification here, frequently using mobile devices. Token-based authentication is another powerful weapon in the security toolbox. The system issues a token or a string of numbers for each transaction using this method. It is challenging hackers to gain unauthorized access to these tokens because of their constantly changing nature (Karim et al., 2021).

Online payment systems frequently need help to strike the right balance between user convenience and security despite the strict measures. Although they provide increased security, users can occasionally see techniques like biometrics as intrusive or burdensome (Ogbanufe & Kim, 2018). Another area for improvement is posed by quantum computing. The development of quantum-resistant algorithms is required because, with its introduction, traditional cryptographic techniques may become vulnerable (Mavroeidis et al., 2018). Stakeholders, including banks, finance companies, and payment platforms, must exercise caution as online payment gateways develop. To ensure the seamless intersection of convenience, privacy, and security, they must be proactive, anticipating potential challenges, and constantly innovating.

4. AI and Blockchain in Online Payment

Due to the rapid convergence of technology, online payments have undergone significant changes recently. Blockchain and Artificial Intelligence (AI) are two of the ground-breaking technologies that are reshaping the financial sector. The blending of Blockchain, cryptocurrency, and AI in finance has ushered in a new era, according to An, Choi, and Huang (2021), highlighting the depth and breadth of potential transformations.

Online payments using AI and Blockchain technology are a significant step forward for digital commerce, providing increased security, effectiveness, and creativity. The need to handle the intricate issues of the digital economy, such as data security, transaction transparency, and user experience optimization, motivates this integration. Blockchain technology and AI offer a strong security foundation for online payments. According to research by Xuan and Ness (2023) and Swan (2018), Blockchain's decentralized structure guarantees that transaction records are transparent and unchangeable, significantly lowering the risk of fraud and data breaches. As Harris and Waggoner (2019) discussed, AI enhances this by offering sophisticated analytics and machine learning algorithms to identify and stop fraudulent activity in real time. This combination increases user trust while also securing transactions.

Innovative business models and improved operational efficiency result from using AI and Blockchain in online payments. In order to make e-commerce platforms more effective and user-friendly, Wang et al. (2022) and Li (2020) explore how AI algorithms can optimize transaction processes, forecast market trends, and personalize customer experiences. Blockchain technology improves overall business performance by expediting settlement times, cutting transaction costs, and streamlining payment procedures. Despite the advantages, the use of AI and Blockchain in online payments has its challenges. The decentralized ledger of Blockchain can result in longer transaction processing times, which is one of the main problems, particularly for large-scale operations. Furthermore, larger businesses may need help developing and integrating AI and Blockchain due to the high technical expertise and resource requirements. Sgantzos and Grigg (2019) have brought attention to concerns regarding data privacy and regulatory compliance. User data should be protected, and these technologies must be implemented to comply with current legal frameworks.

To summarise, the amalgamation of artificial intelligence and blockchain technology in online payments presents a revolutionary strategy for digital transaction management, security augmentation, business innovation stimulation, and operational efficiency improvement. However, in the constantly changing world of digital payments, overcoming the obstacles of scalability, technical complexity, and regulatory compliance is essential to successfully adopting these technologies.

4.1 Security and Trustworthiness of Transactions

Security is one of the main issues with online payments. According to Harris and Waggoner (2019), blockchain technology offers a decentralized and immutable ledger system by its design, ensuring transaction transparency and lowering fraud. When combined with AI, the system can anticipate, recognize, and thwart fraudulent activities in real-time. Algorithms powered by AI analyze patterns, spot anomalies, and even foretell suspicious activity. In their discussion of the convergence of Blockchain, IoT, and AI in 2020, Sandner, Gross, and Richter strongly emphasized the added security that these integrations provide for online transactions.

4.2 Optimizing E-commerce and Improving Efficiency

Integrating blockchain and AI aims to improve user experience, operations efficiency, and security. Li (2020) talked about the structure optimization of blockchain- and AI-based e-commerce platforms, showing how these technologies can result in transaction that is more effective processing, individualized user experiences, and lower operational costs. While blockchain ensures transparency and immutability, AI quickly analyzes enormous amounts of data, speeding up transaction processing.

4.3 The Convergence and Future of Finance

Arslanian and Fischer (2019) provided some insights into the broader implications of developments in FinTech, particularly the impact that AI and cryptocurrency have had on the financial services industry. Their research demonstrates that AI has the potential to handle complex financial tasks, such as risk assessment and predictive analytics. In contrast, the decentralized nature of blockchain technology has the potential to rethink how people trust online payment systems. In addition, Gulati et al. (2020) emphasized the potential future directions of combining blockchain technology with artificial intelligence, which suggests a synchronized synergy that has the potential to revolutionize financial ecosystems.

4.4 Facilitating Big Data and Decision Making

Due to their digital nature, online payments produce tremendous data. When discussing "Big-crypto," Hassani, Huang, and Silva (2018) focused on the interactions between big data, blockchain, and cryptocurrency. With its capacity for data processing, AI can examine these enormous datasets to glean insights and improve the user experience. Muheidat et al. (2022) focused on the potential for smarter decision-making and greater online payment efficiency as they explored new ideas using blockchain and big data. According to the literature, incorporating AI and blockchain in online payments represents a paradigm shift. The future of online transactions will be shaped by their convergence, which promises improved security, effectiveness, and a reimagined user experience.

5. Scope of Online payments in Saudi Arabia

In Saudi Arabia, educational attainment is notably high, with a literacy rate reaching 95% as of 2016 (World Bank, 2016). The country also exhibits a significant mobile penetration rate, recorded at 89.5% in a 2020 report by the General Authority for Statistics (GAS, 2020). This technological receptiveness is further evidenced by the high internet usage among the Saudi population, where, as of 2019, 90% of Saudis, totaling approximately 30.26 million, were active internet users, based on data (GAS, 2020; GMI, 2019). Additionally, social media engagement is robust, with 67% of the population actively using at least one platform (GMI, 2019). The embrace of digital technology extends to the banking sector as well. McKinsey (2016) highlighted that between 80% and 90% of surveyed individuals in Saudi Arabia frequently utilize digital banking channels. More specifically, McKinsey (2016) found that 85% of participants engaged in online banking, while 81% used mobile banking services. Furthermore, the same study revealed a considerable openness among Saudi consumers to digital-only banking propositions, with 52% expressing willingness to open accounts with purely digital banks.

6. Challenges and Opportunities for Online Payments

In the presence of online banking and payment platforms in the global world, it is a challenging task to encourage digital payments (Bandar, 2023) due to critical issues with security, trust, and user experience (Bandar, 2023). It is also critical to inform the public about the advantages and practicality of digital payments. There have been a lot of cybercrimes in Saudi Arabia during the past ten years. According to a recent study by IBM, during the pandemic, data breaches in Dubai and Saudi Arabia resulted in a 6% increase in financial impact, with an average cost per breach of $6.93 million (Al Zoubi, 2023). The financial sector in Saudi Arabia is more vulnerable to cybercrime due to the quick transition of financial services to online and mobile banking and inadequate operational strategies. Therefore, financial institutions should implement a cyber-security governance structure (e.g., blockchain, AI) approved by their board and precisely defined to reduce these risks and manage and combat cyber security threats (Al Zoubi, 2023). Regner and Riener (2017) and Garman et al. (2017) state that online payment privacy and security are significant challenges. In countries where consumer data protection is paramount, businesses must balance user

privacy with the desire to lift internet anonymity for revenue generation. Khalilov and Levi (2018) note that anonymity and transaction transparency are disputed in digital cash systems like Bitcoin. As Goldfeder et al. (2017) note, blockchain technologies complicate this, as traditional tracking methods can conflict with cryptocurrency privacy. Balancing user privacy with regulatory compliance in different countries is challenging due to their legal and regulatory environments. Technological and regulatory differences make each country's challenges unique. Secure and privacy-preserving digital payment systems are complex in countries with less developed digital infrastructures, according to Rajendran et al. (2017). In contrast, advanced digital economies focus on managing more sophisticated cybersecurity threats and complying with strict data protection laws. Balgobin et al. (2016) show how payment instruments and financial privacy concerns can affect online purchase behavior across countries, depending on payment infrastructure and public trust in digital transactions. Online payments have significant growth and innovation potential despite these obstacles. Schomakers et al. (2020) suggest creating privacy-preserving data markets to meet user demand for data protection. Countries can tailor solutions to their market needs and regulatory conditions. The changing landscape of online payments allows countries to collaborate and share best practices. Collaborations can create a global approach to online payments that balances security, privacy, and ease of transaction.

Table 1 highlights the dynamic and evolving financial technology landscape (FinTech) in Saudi Arabia, underscoring various challenges and opportunities. Key issues include regulatory and market challenges for FinTech companies, as identified by Bandar (2023), and cybersecurity concerns in financial services, as noted by Al Zoubi (2023). The economic context, such as GDP per capita and internet penetration rates, also plays a crucial role in shaping the FinTech environment, as shown by the World Bank (2020) and GAS (2020) reports. McKinsey & Company's (2016) study on digital banking adoption and Abiliti's (2023) exploration of blockchain technology's potential indicate both the progress and the untapped potential in the region. However, these studies also reveal limitations, including focusing on specific aspects like social media usage (GMI, 2019) and a need for more generalizability beyond the Saudi Arabian. This complex interplay of technological advancement, regulatory frameworks, and market dynamics forms the core of the FinTech sector's evolution in Saudi Arabia and other countries.

Table 1. Systematic review of the literature

Authors	Aim of the study	Independent variables	Dependent variables	Theory	Findings	Research Gaps/ Limitations
Bandar (2023)	Key challenges for fintech companies in Saudi Arabia	Regulatory environment, market dynamics	Fintech company performance and growth in Saudi Arabia	Market adaptation theory	Identified significant regulatory and market-based challenges	Limited to Saudi Arabian context, may not generalize globally
World Bank (2020)	GDP per capita (current US$) - Saudi Arabia	Economic factors	GDP per capita	Not applicable	Provides current GDP per capita data for Saudi Arabia	Data specific to a single year, limited longitudinal analysis
GAS (2020)	Fixed and mobile broadband services and Internet penetration rate in Saudi Arabia	Technological development, infrastructure investment	Internet penetration rate	Diffusion of Innovations Theory	Increased broadband services and Internet penetration	Focuses on statistical data without qualitative analysis
GMI (2019)	Saudi Arabia social media statistics	Social media trends, demographic factors	Social media usage and preferences	Social Identity Theory	Detailed insights into social media usage trends in Saudi Arabia	Limited to social media, doesn't cover broader digital landscape
McKinsey & Company (2016)	Digital banking in the Gulf	Technological advancements, regulatory policies	Digital banking adoption and efficiency	Technology Acceptance Model	Growth in digital banking adoption with potential for further expansion	Geographically confined to the Gulf region, may not apply globally
Al Zoubi (2023)	Cybersecurity challenges in KSA's financial services	Cyber threats, regulatory frameworks	Cybersecurity measures and effectiveness	Cybersecurity Resilience Theory	Highlights significant cybersecurity challenges and mitigation strategies	Specific to KSA's financial sector, limited generalizability

Abiliti (2023)	Embracing blockchain in KSA	Blockchain technology implementation	Transparency, efficiency, and trust in financial services	Blockchain Adoption Model	Positive impact of blockchain on transparency and efficiency	Focuses on potential future impacts, lacks empirical data

Therefore, the theoretical contribution of "AI and Blockchain-based Online Payments: How it is Service Quality Traces Bank Sustainable Performance" lies in linking advanced AI and blockchain technologies in online payments to enhance service quality, which in turn drives sustainable performance in the banking sector. This approach highlights the pivotal role of technological integration in achieving long-term efficiency and customer satisfaction within the financial industry. Therefore, the study will measure the use of AI and blockchain technologies while doing online transactions/payments on different online platforms.

The literature shows that while country-specific factors affect online payment challenges, they also offer tailored innovations and international cooperation opportunities. Advancement of the global online payment ecosystem requires balancing privacy and security, adapting to technological and regulatory diversity, and seizing market-specific solutions.

6.1 Advantages of Blockchain technology

Blockchain technology is revolutionizing transaction recording and validation with significant benefits, including increased fraud protection, reduced costs, and enhanced data integrity (Abiliti, 2023). Its influence is especially apparent in finance, where it guarantees data accuracy and reduces online fraud. In addition, blockchain technology is helping the Kingdom of Saudi Arabia (KSA) achieve its Vision 2030 goals by providing a secure distributed ledger system that eliminates the need for intermediaries in transaction processing (Abiliti, 2023). This technology is essential for protecting businesses and citizens from financial fraud and increasing efficiency, transparency, and security in various industries. Furthermore, blockchain technology is anticipated to boost KSA's economy by generating new job opportunities and improving the nation's economy, particularly in industries like supply chain management, finance, and healthcare.

6.2 Rational contribution

The rational contribution illustrates the possibility of conducting research on the relationship between service quality and technology adoption in Saudi Arabia's online payments by users. The justification for this kind of research stems from an understanding of how combining blockchain technology with artificial intelligence (AI) can improve the caliber of online payment services, potentially resulting in sustainable financial performance. Analyzing these connections is essential in the Saudi Arabian context, where digital transformation is a major tenet of Vision 2030 (McKinsey & Company, 2016). While blockchain might improve online transaction security and trust, artificial intelligence (AI) has the potential to streamline decision-making and customer service. The study will highlight the potential contribution of enhanced service quality, encompassing tangibles such as assurance, responsiveness, reliability, and empathy, to the financial sector's resilience and long-term viability. Through an analysis of these dynamics, the study will seek to shed light on how Saudi Arabia's financial sector can benefit from technological advancements by increasing customer satisfaction and financial viability.

7. Limitations and future directions

Previous literature studies did not focus on AI-based and blockchain-based online payments in Saudi Arabia to sustain the economy. In addition, how the study explores the contextual challenges and barriers in the adoption of online payments due to the lack of advanced technologies, i.e., *'AI' and 'blockchain'*. Therefore, the theoretical contribution of "AI and Blockchain-based Online Payments: How it is Service Quality Traces Bank Sustainable Performance" lies in linking advanced AI and blockchain technologies in online payments to enhance service quality, which in turn drives sustainable performance in the banking sector. This approach highlights the pivotal role of technological integration in achieving long-term efficiency and customer satisfaction within the financial industry.

8. Conclusion

While user intentions can provide insights, the actual utilization of the AI and blockchain in online payments are where tangible outcomes emerge. Thus, bridging the gap between intention and system availability (the availability of AI and blockchain) remains critical for online payment service quality. In the backdrop of this transition lies the potential influence of AI and blockchain. As AI and blockchain become more intertwined with everyday processes, its adoption may be crucial in shifting from mere

intention to actual usage of the technologies. Lastly, at the heart of any service lies its quality. The use of the AI and blockchain in online payment system and its repercussions on service quality will be dissected in this research. Furthermore, in an age where sustainability and responsible practices are gaining prominence, understanding how service quality insights affect sustainable performance in the banking sector can offer invaluable perspectives. *In this research, we compared the strengths and weaknesses of various payment technologies. Our future work involves providing tailored solutions based on the user's needs and the level of security required by the users.*

List of Acronyms

The table below describes the significance of various acronyms used throughout the paper.

Acronym	Meaning
MENA	Middle East and North Africa
AI	Artificial Intelligence
DAM	Decentralized anonymous micropayment
SFC	The stock-flow consistent
B2B	Business-to-business
B2C	Business-to-consumer
C2C	Consumer-to-consumer
EFT	Electronic funds transfer
MPS	Mobile payment services
KSA	The Kingdom of Saudi Arabia
FinTech	Financial Technology

References

[1] Abiliti. (2023, May 29). Embracing blockchain: A future of enhanced transparency, efficiency, and trust in KSA. *Born in Riyadh, Bred in Innovation*. https://www.linkedin.com/pulse/embracing-blockchain-future-enhanced-transparency-efficiency Agarwal, S., & Zhang, J. (2020). FinTech, lending and payment innovation: A review. *Asia-Pacific Journal of Financial Studies*, *49*(3), 353-367.

[2] Al Zoubi, A. (2023, April 1). Cyber security challenges facing KSA's financial services. *GrantThornton.* https://www.grantthornton.sa/en/insights/articles-and-publications/cyber_security_in_financial_institutes/

[3] An, Y. J., Choi, P. M. S., & Huang, S. H. (2021). Blockchain, cryptocurrency, and artificial intelligence in finance. In *Fintech with artificial intelligence, big data, and blockchain* (pp. 1-34). Singapore: Springer Singapore.

[4] Arslanian, H., & Fischer, F. (2019). *The future of finance: The impact of FinTech, AI, and crypto on financial services*. Springer.

[5] Balgobin, Y., Bounie, D., Quinn, M., & Waelbroeck, P. (2016). Payment instruments, financial privacy and online purchases. *Review of Network Economics*, *15*(3), 147-168.

[6] Bandar, A. (2023, October 12). Key challenges for fintech companies in Saudi Arabia. *Majd Alaamal Payments.* https://www.linkedin.com/pulse/key-challenges-fintech-companies-saudi-arabia-bandar-alnuhayr-veelf

[7] Berentsen, A. (2019). Aleksander berentsen recommends "bitcoin: a peer-to-peer electronic cash system" by Satoshi Nakamoto. *21st Century Economics: Economic Ideas You Should Read and Remember*, 7-8.

[8] Chiesa, A., Green, M., Liu, J., Miao, P., Miers, I., & Mishra, P. (2017). Decentralized anonymous micropayments. In *Advances in Cryptology–EUROCRYPT 2017: 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30–May 4, 2017, Proceedings, Part II 36* (pp. 609-642). Springer International Publishing.

[9] De Luna, I. R., Liébana-Cabanillas, F., Sánchez-Fernández, J., & Muñoz-Leiva, F. (2019). Mobile payment is not all the same: The adoption of mobile payment systems depending on the technology applied. *Technological Forecasting and Social Change*, *146*, 931-944.

[10] Decker, C., & Wattenhofer, R. (2015). A fast and scalable payment network with bitcoin duplex micropayment channels. In *Stabilization, Safety, and Security of Distributed Systems: 17th International Symposium, SSS 2015, Edmonton, AB, Canada, August 18-21, 2015, Proceedings 17* (pp. 3-18). Springer International Publishing.

[11] Ducas, E., & Wilner, A. (2017). The security and financial implications of blockchain technologies: Regulating emerging technologies in Canada. *International Journal*, *72*(4), 538-562.

[12] Garman, C., Green, M., & Miers, I. (2017). Accountable privacy for decentralized anonymous payments. In *Financial Cryptography and Data Security: 20th International Conference, FC 2016, Christ Church, Barbados, February 22–26, 2016, Revised Selected Papers 20* (pp. 81-98). Springer Berlin Heidelberg.

[13] General Authority for Statistics (GAS). (2020). Fixed and mobile broadband services and Internet penetration rate. Retrieved August 15, 2020, from https://www.stats.gov.sa/en/6390

[14] Giudici, P. (2018). Fintech risk management: A research challenge for artificial intelligence in finance. *Frontiers in Artificial Intelligence*, *1*, 1.

[15] Global Media Insight (GMI). (2019). Saudi Arabia social media statistics 2019 (Infographics) - GMI Blog. Retrieved September 15, 2020, from https://www.globalmediainsight.com/blog/saudi-arabia-social-media-statistics/

[16] Goldfeder, S., Kalodner, H., Reisman, D., & Narayanan, A. (2017). When the cookie meets the blockchain: Privacy risks

of web payments via cryptocurrencies. *arXiv preprint arXiv:1708.04748*.

[17] Gomber, P., Koch, J. A., & Siering, M. (2017). Digital Finance and FinTech: current research and future research directions. *Journal of Business Economics*, *87*, 537-580.

[18] Gulati, P., Sharma, A., Bhasin, K., & Azad, C. (2020, May). Approaches of blockchain with ai: Challenges & future direction. In *Proceedings of the international conference on innovative computing & communications (ICICC)*.

[19] Harris, J. D., & Waggoner, B. (2019, July). Decentralized and collaborative AI on blockchain. In *2019 IEEE international conference on blockchain (Blockchain)* (pp. 368-375). IEEE.

[20] Harris, J. D., & Waggoner, B. (2019, July). Decentralized and collaborative AI on blockchain. In *2019 IEEE international conference on blockchain (Blockchain)* (pp. 368-375). IEEE.

[21] Hassani, H., Huang, X., & Silva, E. (2018). Big-crypto: Big data, blockchain and cryptocurrency. *Big Data and Cognitive Computing*, *2*(4), 34.

[22] Heilman, E., Baldimtsi, F., & Goldberg, S. (2016, February). Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions. In *International conference on financial cryptography and data security* (pp. 43-60). Berlin, Heidelberg: Springer Berlin Heidelberg.

[23] Huang, R., Tlili, A., Wang, H., Shi, Y., Bonk, C. J., Yang, J., & Burgos, D. (2021). Emergence of the online-merge-offline (OMO) learning wave in the post-COVID-19 era: a pilot study. *Sustainability*, *13*(6), 3512.

[24] Jiang, Q., Ma, J., Li, G., & Li, X. (2015). Improvement of robust smart-card-based password authentication scheme. *International Journal of Communication Systems*, *28*(2), 383-393.

[25] Karim, R., Rumi, L. S., Ashiqul Islam, M., Kobita, A. A., Tabassum, T., & Sagar Hossen, M. (2021). Digital signature authentication for a bank using asymmetric key cryptography algorithm and token based encryption. In *Evolutionary Computing and Mobile Sustainable Networks: Proceedings of ICECMSN 2020* (pp. 853-859). Springer Singapore.

[26] Khalilov, M. C. K., & Levi, A. (2018). A survey on anonymity and privacy in bitcoin-like digital cash systems. *IEEE Communications Surveys & Tutorials*, *20*(3), 2543-2585.

[27] Kumar, V., Lai, K. K., Chang, Y. H., Bhatt, P. C., & Su, F. P. (2021). A structural analysis approach to identify technology innovation and evolution path: a case of m-payment technology ecosystem. *Journal of Knowledge Management*, *25*(2), 477-499.

[28] Li, S. (2020). Structure optimization of e-commerce platform based on artificial intelligence and blockchain technology. *Wireless Communications and Mobile Computing*, *2020*, 1-8.

[29] Li, S. (2020). Structure optimization of e-commerce platform based on artificial intelligence and blockchain technology. *Wireless Communications and Mobile Computing*, *2020*, 1-8.

[30] Liébana-Cabanillas, F., Muñoz-Leiva, F., Molinillo, S., & Higueras-Castillo, E. (2022). Do biometric payment systems work during the COVID-19 pandemic? Insights from the Spanish users' viewpoint. *Financial Innovation*, *8*(1), 1-25.

[31] Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. *arXiv preprint arXiv:1804.00200*.

[32] McKinsey & Company. (2016). Digital banking in the Gulf. Retrieved October 1, 2020, from https://www.mckinsey.com/~/media/mckinsey/locations/europe%20and%20middle%20east/middle%20east/overview/insights/digital%20banking%20in%20the%20gulf/digital%20banking%20in%20the%20gulf%20161116%20digital.ashx

[33] Muheidat, F., Patel, D., Tammisetty, S., Lo'ai, A. T., & Tawalbeh, M. (2022). Emerging concepts using blockchain and big data. *Procedia Computer Science*, *198*, 15-22.

[34] Nikiforos, M., & Zezza, G. (2018). Stock-Flow Consistent macroeconomic models: a survey. *Analytical Political Economy*, 63-102.

[35] Ogbanufe, O., & Kim, D. J. (2018). Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment. *Decision Support Systems*, *106*, 1-14.

[36] Oo, K. Z. (2019). Design and implementation of electronic payment gateway for secure online payment system. *Int. J. Trend Sci. Res. Dev*, *3*, 1329-1334.

[37] Puspadini, M., Yudhapramesti, P., & Bakry, G. N. (2023). Visitor Motives of Interest in Using DailySocial. id as a Micropayment News Portal. *Jurnal Kajian Jurnalisme*, *6*(2), 171-184.

[38] Rajendran, B., Pandey, A. K., & Bindhumadhava, B. S. (2017, August). Secure and privacy preserving digital payment. In *2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)* (pp. 1-5). IEEE.

[39] Regner, T., & Riener, G. (2017). Privacy is precious: On the attempt to lift anonymity on the internet to increase revenue. *Journal of Economics & Management Strategy*, *26*(2), 318-336.

[40] Rußell, R., Berger, B., Stich, L., Hess, T., & Spann, M. (2020). Monetizing online content: Digital paywall design and configuration. *Business & Information Systems Engineering*, *62*, 253-260.

[41] Sandner, P., Gross, J., & Richter, R. (2020). Convergence of blockchain, IoT, and AI. *Frontiers in Blockchain*, *3*, 522600.

[42] Schomakers, E. M., Lidynia, C., & Ziefle, M. (2020). All of me? Users' preferences for privacy-preserving data markets and the importance of anonymity. *Electronic Markets*, *30*, 649-665.

[43] Sgantzos, K., & Grigg, I. (2019). Artificial intelligence implementations on the blockchain. Use cases and future applications. *Future Internet*, *11*(8), 170.

[44] Sinha, N., & Singh, N. (2023). Moderating and mediating effect of perceived experience on merchant's behavioral intention to use mobile payments services. *Journal of Financial Services Marketing*, *28*(3), 448-465.

[45] Swan, M. (2018). Blockchain for business: Next-generation enterprise artificial intelligence systems. In *Advances in computers* (Vol. 111, pp. 121-162). Elsevier.

[46] Talib, A. A., & Salman, A. D. (2022). Design and develop authentication in electronic payment systems based on IoT and biometric. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, *20*(6), 1297-1306.

[47] Wang, Z., Li, M., Lu, J., & Cheng, X. (2022). Business Innovation based on artificial intelligence and Blockchain technology. *Information Processing & Management*, *59*(1), 102759.
[48] World Bank. (2020). GDP per capita (current US$) - Saudi Arabia. Retrieved October 13, 2020, from https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=SA
[49] Xuan, T. R., & Ness, S. (2023). Integration of Blockchain and AI: Exploring Application in the Digital Business. *Journal of Engineering Research and Reports*, *25*(8), 20-39.

Authors

Dr. Prakash Veeraraghavan
Assoc Prof, Comp Sci and IT, Computer Science & Information Technolog

Dr. Dalal Hanna
Lecturer, Computer Science, and IT (TF), Computer Science & Information Technology

Ahlam Alhalafi
PhD Student at La Trobe University, Computer Science & Information Technology Department.