



ADGM
Academy

RESEARCH
CENTRE

DIGITAL PAYMENTS IN THE UAE:
**CURRENT LANDSCAPE,
LESSONS LEARNED AND
OPPORTUNITIES FOR
FUTURE GROWTH USING
BLOCKCHAIN**

EXECUTIVE SUMMARY

AUTHORED BY:

JAYAPRADA PUTREVU – ABU DHABI UNIVERSITY

MUNA AL SUWAIDI – ABU DHABI UNIVERSITY

SALWA AL BREIKI – ABU DHABI SCHOOL OF MANAGEMENT

COMMISSIONED BY

ADGM ACADEMY RESEARCH CENTRE

The ADGM Academy Research Centre commissioned a team of university students to explore the emergence and importance of digital payments in the UAE economy. Jayaprada and Muna from Abu Dhabi University and Salwa from the Abu Dhabi School of Management undertook this research as they embarked on their own exploration to understand digital payments. In this paper they provide an overview of the global landscape of digital payments as well as the UAEs journey of digital transformation.

They explore both the opportunities and challenges that a digital environment presents and define the optimal infrastructure necessary to support digital payments. They take a close look at the role of blockchain and conclude with a six-step process for introducing a digital payments system into an economy.

We thank Jayaprada, Muna and Salwa for their tireless efforts and are proud to publish this research paper on their behalf.

We thank Andrew McCollum, Senior Manager, Banking & Insurance Authorisation, ADGM Financial Services Regulatory Authority, for his support and guidance of the students throughout this project.

AUTHOR ACKNOWLEDGEMENTS

Professor Charilaos Mertzanis is a professor of finance in Abu Dhabi University. His current research interests include the role of institutions in corporate decision-making across countries and the effect of crises episodes on global financial transactions.

Dr. Charilaos Mertzanis, you have been an excellent guide, and we want to convey our gratitude for all you've done in helping us to accomplish this white paper, despite your own busy schedule.

We would like to thank ADGM Academy for giving us this opportunity to research and write this paper. Nothing would have been possible without the handholding of Jassim Yehya Mohamed AlMarzooqi, Associate Director, Business Enablement of the Academy, who has been an immense support during our journey at the academy.

Lastly but the most crucial person, Peter Ware, Head of Research and Development of the Academy, who has been with us on this journey in a very unique way. Thank you so much for taking the time to provide us with constructive criticism and for taking an interest in our progress.

DIGITAL PAYMENT SERVICES LANDSCAPE



Financial technology and digital payment services have prompted policymakers globally to consider their financial stability benefits and risks. Payments, clearing and settlement are activities where material service developments have rapidly evolved. This includes retail and wholesale, large-value, and cross-border payments. So far changes in the retail payment space are among the most visible. The key drivers include the promotion of cashless transactions, competition, financial inclusion, financial integration, and innovation to address banking relationships. Despite the small size of digital payment services relative to the financial system as a whole, growth in such activities and the supervisory and regulatory issues have attracted policy attention.



Authorities regulate payments systems and service providers to maintain the integrity of the monetary system, safeguard financial stability by ensuring final settlement of monetary transfers, and protect financial consumers. The impact of digital payment services on financial system growth and stability may be affected by the market entrance of large technology (e.g. BigTech) firms into payment services. As the market structure evolves, advances in digital payment services indicate that regulatory frameworks and their legal foundations must shift from entity-based to activity-based regulation.

Financial regulation has traditionally been based on the regulation of types of entities or intermediaries performing broad functions, such as payments systems. Licensing regimes will need to be redesigned to bring new types of service providers within the regulatory perimeter, where appropriate, including digital payment services and BigTech.

The first step of a digital payment framework is to identify if an economic activity undertaken by the entity is a payment service. The proper identification of payment activities helps to design effective oversight and supervisory frameworks, while avoiding unnecessary overlaps and/or duplication of regulatory efforts. International best practices suggest that such activities could be organized into six general groups:

- account issuance
- electronic money issuance
- domestic funds transfer
- cross-border funds transfer
- merchant acquisition
- digital payment tokens

These primarily relate to services delivered to payment-service users rather than the payments systems themselves.

Value of Digital Payments

Globally the digital payments market had a transaction value of USD \$5.4 trillion in 2021.

China was the biggest market with a transaction value of USD \$2.9 trillion, followed by the USA with USD \$1.5 trillion and the UK with USD \$352 billion). In the MENA region in 2021 Saudi Arabia was the largest market (USD \$24.9 billion), followed by the UAE (USD \$18.1 billion).



Value of digital payments, realized and projected, in selected countries (USD bn)

COUNTRY	2017	2018	2019	2020	2021	2022*	2023*	2024*	2025*	2026*
Panel A. MENA										
Algeria	1.326	1.744	2.413	2.844	3.666	4.272	4.847	5.332	5.788	6.292
Bahrain	0.861	0.942	1.048	1.253	1.463	1.727	1.938	2.167	2.401	2.596
Egypt	4.311	4.574	5.948	8.064	11.64	14.07	16.14	18.09	20.1	22.45
Iran	5.326	6.929	8.826	11.93	17.81	21.54	26.38	32.95	41.17	51.7
Iraq	2.181	3.173	4.23	5.209	6.348	7.643	9.119	10.65	12.32	14.17
Israel	5.266	6.275	7.713	9.451	14.64	19.4	24.77	31.04	37.68	43.77
Jordan	1.332	1.854	2.518	3.887	5.117	6.238	7.377	8.524	9.753	11.12
Kuwait	3.262	3.909	4.761	6.129	8.024	10.08	12.43	14.81	17.42	20.28
Lebanon	1.894	2.079	2.3	2.785	3.463	4.203	4.858	5.538	6.238	6.982
Morocco	2.102	2.5	2.832	2.965	3.93	4.874	5.814	6.771	7.743	8.744
Oman	1.512	1.871	2.444	3.698	5.124	6.514	7.932	9.445	11.07	12.85
Qatar	2.746	3.113	3.424	3.79	4.534	5.457	6.425	7.334	8.294	9.285
Saudi Arabia	8.898	12.12	15.85	19.76	24.98	30.66	36.28	42.06	48.04	54.46
UAE	7.269	8.858	10.65	13.71	18.12	20.15	22	23.95	26.05	28.41
Panel B. Other Countries										
Singapore	4.038	5.196	6.748	8.614	13.43	17.18	21.68	26.7	32.3	38.37
Malaysia	4.843	6.704	8.424	9.664	14.38	18.22	22.34	27.04	32.2	37.9
India	42.16	51.3	66.79	88.52	116.9	137.4	158.8	181.1	205.7	233.7
Indonesia	13.63	19.26	28.5	40.01	62.92	71.41	80.15	89.71	100.5	113
China	1360	1754	1989	2568	2997	3318	3645	3952	4292	4666
UK	172.9	198.2	214	269.3	352.5	436.4	514.2	596.2	685.6	782.1
USA	740.1	867.5	1019	1252	1527	1801	2090	2417	2787	3200

Source: Digital payments report, 2021, Statista

* Indicates estimated values.

THE UAE'S DIGITAL TRANSFORMATION



The UAE has exhibited considerable transformation in recent years. As of 2019, ICT (information and communications technology) spending in the UAE increased considerably. The telecom services sector accounted for the highest spending, at 8.77 billion U.S. dollars, which was around half of the country's total ICT spending in the same year.

Furthermore, the share of digital transformation adoption among institutions also changed. As of 2019, 34% of firms had a company-wide digital transformation strategy already in implementation. 90% of firms were undergoing digital transformation initiatives, and 61% were running a company-wide digital transformation strategy.

The UAE has a highly banked population with 83% along with 37% card penetration. The country has one of the world's highest smartphone penetration levels (78%), a significant factor contributing to the fast-rising use of digital payments.

The distribution of digital payment methods for e-commerce transactions in the UAE shows considerable diversification. As of 2020, the most popular online payment method was by card at approximately 49%, followed by e-wallets at 18%.



DIGITAL PAYMENTS CHALLENGES



The digitisation of payment services brings significant benefit and presents many opportunities, but there are challenges to overcome.

Financial Crime and Cybersecurity

- Consumers data information has greater exposure to potential risks of account hacking, money laundering and fraud
- Cybersecurity threats are increasing as the digitisation of payments expands; customer data is open to malicious attacks due to unauthorized access

Speed and efficiency of transactions

- Consumer demand for faster / immediate payment is continually increasing
- End-users demand confirmation that their transaction is complete
- Fast and efficient digital payments require technology advancement and infrastructure, thus increased investment costs for intermediaries and payment service providers

The organization of fast payment provision

- How the digital payment industry organizes faster payment systems (e.g. as a single or multiple systems, or closed vs open systems) affects the level of coordination and nature of competition
- Where multiple systems are used a key issue of interoperability; systems must be compatible and interoperable to offer the best service to the end-user

Clearing and settlement issues

- Although both real-time and deferred clearing and settlement can support faster payments, the various clearing and settlement methods between payment service providers could result in diverging outcomes in terms of risk and efficiency
- Verifying payment requests is a challenge due to a reliance on virtual communication for payment initiation

Ease of access / financial inclusion

- Today financial inclusion is a critical issue for billions of people around the world
- Advancement and innovation in digital technologies will pave the way to improve financial inclusion, thereby enabling digital payments for many people who have no payment capabilities today

TECHNOLOGY DEVELOPMENTS & INFRASTRUCTURE

The payment methodology used in most countries evolved from early banking payments systems and still retains structural characteristics from those roots. By trading inherently valued objects such as gold coins, early payments were made. When goldsmith banks first appeared in the 1600s, they kept records of the money their clients deposited, making it possible to make payments by adjusting the records rather than physically swapping the assets. Only clients of the same bank could use this. Over time, the need to make inter-bank payments led to the emergence of a central clearing bank through which member banks could hold accounts, making interbank payments simpler.



In standard payment systems, payments are facilitated by reducing the balance in a customer's account and increasing the balance in the user's account by the same amount. Technological developments over the past several decades have impacted payments systems in two major ways.

- First, the records and ledgers have moved from paper to electronic form, thereby increasing the speed of transactions and reducing operational risks.
- Second, the emergence of cheaper and faster technology has enabled new payment schemes to emerge (e.g. mobile money schemes).

Regardless of the use of new technology, the basic structure of centralized payment systems remains unchanged. A central ledger is at its core, and settlement occurs across the books of an organisation that serves as a clearing point (a function typically carried out by the central bank). Each participant to a transaction, usually a commercial financial institution, holds a balance at the central bank, which is recorded in the latter's ledger, and also reflected in the participant bank's own (internal) ledger. Individual customers, branches, or even other (smaller) banks hold balances at the participant bank, which would again be recorded in their own ledger.

In areas where access to traditional banking infrastructure is limited, development and adoption of new payments systems serve to fulfil unmet demand. In more developed economies, new payments systems are probably developed in response to the high operational margins associated with incumbent systems and adopted based on their ease of use. The development of mobile money schemes represents new payment systems with money stored as credit on a smart card or a system-provider's books, while continuing to use national currencies (e.g. M-Pesa in Kenya, which grants access to financial services to anyone with a mobile phone).

The development of the distributed ledger ('blockchain') is a key technical innovation underlying the emergence of digital currencies that solves the problem of 'double spend' in a decentralized payments system. It rests on concepts originating in cryptography, peer-to-peer networking and game theory. A key problem for any electronic payments system is to ensure that money cannot be spent twice. If a payee has a single \$1-coin, s/he cannot pay the \$1 both to counterparty 1 and also counterparty 2. The physical act of exchange prevents the payer from spending the same money twice. In a payments system that relies on digital exchange, records must have a way of preventing double spending, since it is easy to do that by copying and editing digital records.

Regardless of the technology or framework in place, innovative digital payment mechanisms require the development of reliable and efficient infrastructures to offer user-friendly, secure, and cost-effective services. Such infrastructures have the potential to increase financial access, expand financial inclusion and support the digital payments system.

THE ROLE OF BLOCKCHAIN AND CYBERSECURITY



Digitisation of any process requires technology. While technology provides process automation, reduces manual processing errors, and speeds up processing times, it also presents opportunities for new cyber risks.

Cybersecurity vulnerability threats advance at the same pace as new technology developments. Considering the complexity and risk associated, there is an urgent need to protect the entire digital payments system. Because of the development of sophisticated ransomware and the growing threat posed by specialized cyber organizations, cyberattacks have grown increasingly complex. In addition to the potential benefits of increased transparency and speed, blockchain-based solutions are gaining momentum because of their potential to mitigate cyber-attacks. Both controlled and decentralized blockchains are possible. It's crucial, though, to distinguish decentralized from distributed. A blockchain is intrinsically distributed but is not inherently decentralized (multiple parties retain copies of the ledger). The rights of members on the ledger determine if a blockchain is centralized or decentralized, hence this is a design feature, Anyone can join in and conduct transactions on the ledger in a decentralized network.



To protect against the flaws in this architecture and guarantee that transactions are accurate, measures must be in place. Blockchains that are decentralized, like Bitcoin, are common. Parties in a centralized network are those whose identities are recognized. Because only trustworthy and respected individuals are allowed to post to the ledger, the system is therefore legitimate. Participants' transactions may be audited because it is known who they are. To reduce vulnerability, a centralized distributed ledger must be utilized in any tightly regulated industry, such as financial services.



Authentication and authorization control

- A typical problem for organizations is limiting access to the right task to the right people
- In a publicly available blockchain, there is no need to control network access as everyone has the right to participate and access the entire network
- In contrast, private blockchains need robust security measures in place to prevent unwanted users from gaining access to the network
- In the face of cyberattacks proper encryption-driven authorization will prevent reading or retrieving information stored on the blockchain network
- Use of threat intelligence
- Threat intelligence involves acquiring information about a cyber threat
- A major obstacle, however, is that providers of digital services spend significant time researching the same threats, while others are left unnoticed
- Blockchain, with its peer-to-peer oriented architecture, could help in maintaining synchronization between different parties, thereby transforming the threat intelligence process
- Blockchains decentralized infrastructure also acts as an anti-tampering structure that helps detect everything in real-time



Data consistency and integrity

- Data integrity can be maintained as a result of a blockchains immutability and transparency
- Blockchain technology makes use of sequential hashing and cryptography, making data tampering almost impossible
- The technology ensures that records are digitally signed and time-stamped, implying that users can trace back each transaction and identify the corresponding party whenever required
- Blockchain technology also serves to ensure non-repudiation (e.g. transactions are undeniable)



Accuracy and quality of information

- Blockchains help to ensure accuracy and maintain the quality of information
- While it cannot guarantee or enhance data quality, blockchains are responsible for maintaining data accuracy and durability after it has been entered into the ledger



Timely and reliable access

- DDoS (distributed denial of service) cyberattacks focus on disrupting the availability of internet services
- DDoS attacks on blockchains, however, are not usual occurrences as they are too costly (e.g. trying to defeat the entire blockchain comprising large volumes of small transactions)



CONCLUSION AND WAY FORWARD



The adoption of digital payments offers several benefits including greater speed, efficiency, higher transparency and security of transactions, expanded financial inclusion opportunities that extend to women and social minorities, and broader economic growth and poverty reduction. To achieve these benefits, the introduction of a digital payments system must take place responsibly and in ways that protect and promote the well-being of end-users.

Digital Payment Framework

- STEP 01** Identify the range and nature of payment activities that shall be designated as digital payments, subject to effective monitoring and oversight while avoiding unnecessary overlaps and/or duplication of regulatory efforts.
- STEP 02** Introduce a proper and efficient infrastructure that provides the basis for offering user-friendly, secure, and cost-effective services.
- STEP 03** Identify the causes that might limit the active use of digital payment technologies based on the users' experiences and perceptions of associated digital payment risks.
- STEP 04** Contextualize and understand the nature, incidence, and consequences of digital consumer risks. Adhering to the basic principles of data/process reliability, communication, and monitoring provides the core background for policy development to mitigate digital payment risks.
- STEP 05** Develop specific policy interventions that ensure the reliability of the payments experience making the customer interface user-friendly, ensuring agent service quality, training, and digital liquidity management, as well as effective risk mitigation governance.
- STEP 06** Explore the benefits of new technologies and especially the role of blockchain for mitigating digital consumer risks. Due to its immutable, and transparent nature, blockchains could improve cyber defence and prevent fraudulent activities.

Blockchains have surfaced as a remarkable technology in the field of information technology. Increasing acceptance of cryptocurrencies is one of the primary reasons driving market expansion. Banks globally are utilizing blockchain technology to process payments.

However, the fragmented acceptance of blockchain comes with its own range of obstacles that can impede its operation, such as higher costs, failed standards, and a lack of interoperability. Interoperability is necessary for the easy integration of blockchain payments into existing systems. To address this a concentrated effort must be placed on a small number of components, such as improvement of network scale efficiency and the deployment of a standard form of communication.

When transitioning from one technological solution to another, there will always be obstacles to overcome. As blockchain in finance is still a developing business, it is normal to encounter a few issues and concerns. However, with the right measures and care, one may swiftly overcome these obstacles and proceed on to relish the technology's many benefits.



ABOUT *ADGM ACADEMY*

ADGM Academy is part of Abu Dhabi Global Market (ADGM), an International Financial Centre (IFC) located in the capital city of the United Arab Emirates. The Academy has been established with the vision of becoming one of the leading academies in the region, providing world-class financial research and training services.

Delivering world-class financial education and literacy, ADGM Academy will help to position Abu Dhabi as a leading global financial centre. This will be achieved through globally recognised educational and experiential programmes on a range of topics and qualifications in banking, finance, leadership, entrepreneurship, technical and soft skills.

ABOUT *RESEARCH CENTRE*

The ADGM Academy Research Centre brings together an ecosystem of academics, financial industry practitioners, government and technology experts to unlock the shared potential to improve the financial environment in MENA and beyond.

The financial industry continues to transform at a rapid pace with new technologies, disruptors, threats and opportunities appearing all the time. Independent research is crucial to be able to understand and utilise this transformation for the benefit of your business, your customers and society in general.

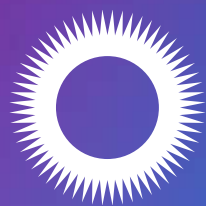
The Research Centre provides that understanding through insights developed in collaboration with the academic community.

STAY UP TO DATE WITH ADGM ACADEMY RESEARCH CENTRE.

📍 adgmacademy.com ✉ research@adgm.com

FOLLOW US
ON OUR SOCIAL NETWORKS





ADGM
Academy

RESEARCH
CENTRE

DIGITAL PAYMENTS IN THE UAE

ADGM Academy Abu Dhabi Global Market
Level 20, Al Maqam Tower
ADGM Square, Al Maryah Island
PO Box 111999 – Abu Dhabi, UAE
T : +971 2 333 8500