

Middle East

Point of View

Published by Deloitte & Touche (M.E.) and distributed to thought leaders across the region | Summer 2023

The darker side of GenAI

Being aware and mitigating risks

Too green to be true?

A greenwashing overview

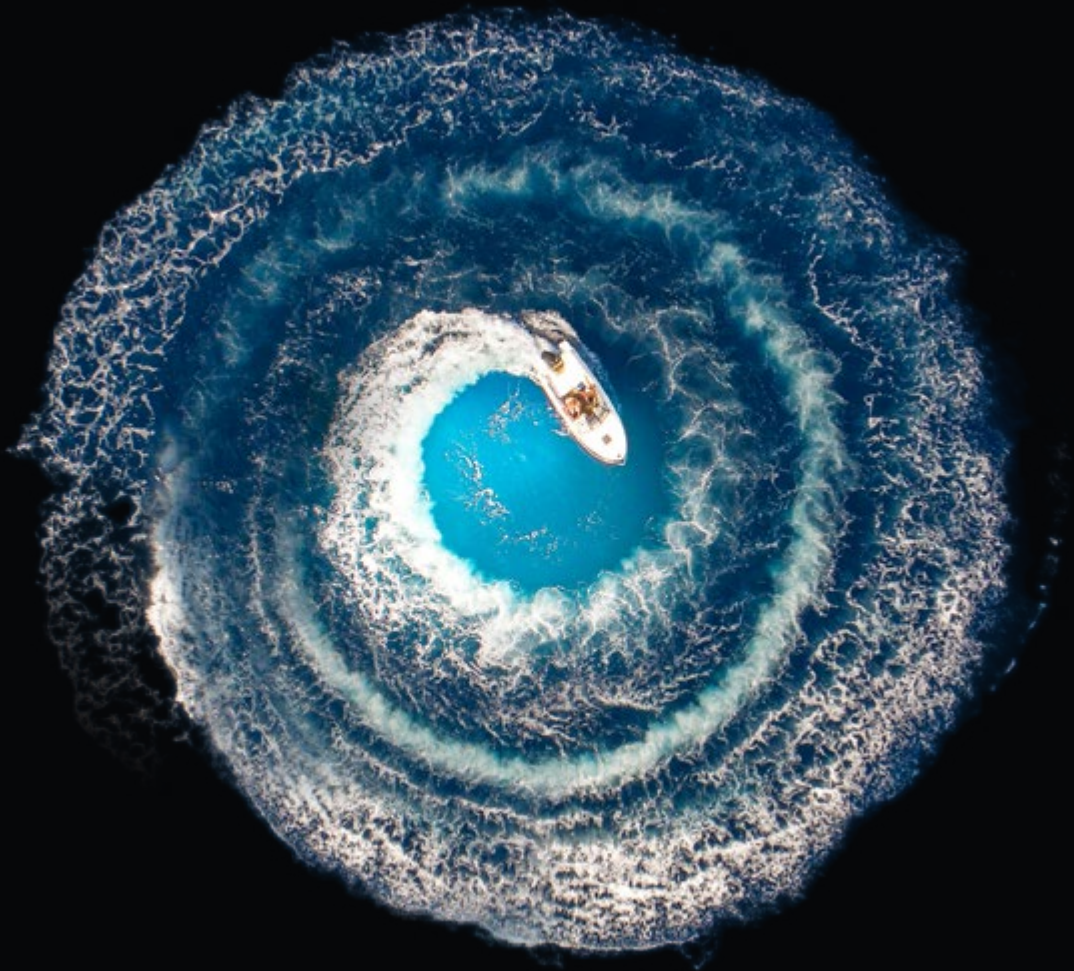
The e-commerce landscape

How the Middle East is thriving

IoT and blockchain integration

For the sake of cyber safety

Swift moves



Deloitte.

MAKING AN
IMPACT THAT
MATTERS

since 1845

Summer 2023
Middle East Point of View
Published by Deloitte & Touche (M.E.)

www.deloitte.com/middleeast

A word from the editorial team

In the bustling realm of Middle Eastern business, where opportunity dances hand-in-hand with ambition, one must balance out their "swift moves." And since the business landscape in this region is marked by a relentless pace and a fervent quest for growth, it takes such swift moves to keep up with the tempo.

Economic growth in the region is palpable. In his article *The thriving e-commerce landscape in the Middle East*, Dr. Ahmed Hezzah shows how with advancements in technology, changing consumer behavior, and increased internet penetration, e-commerce has emerged as a key driver of economic growth in the region. In *The evolving role of finance post IPOs: Shaping the future of finance and the UAE capital markets*, Farhad Aklas and Nav Dulay weigh in on the dynamics of the economic landscape and how the UAE has emerged as a prominent destination for initial public offerings (IPOs), reflecting the country's commitment to foster a robust capital market and attract global investment.

In Humaid Hussain and Khushnood Khan's article *Is artificial intelligence the new benchmark for financial crime risk management?* it becomes apparent how the game of cat and mouse between criminals and regulators has reached unprecedented levels. While the synergistic partnership between AI and financial institutions brings hope for a safer financial landscape, it also raises concerns about the ethical implications of such power. *On high alert: The darker side of generative AI*, by Ralph Stobwasser and Nicki Koller, emphasizes how in order to mitigate the risks of generative AI, individuals and organizations should drive awareness of these risks alongside the benefits in order to move forward.

As the swift moves of generative AI continue to shape our world, it becomes crucial to address the intricacies of our digital age, according to Govinda Mengji in the article *Integrating IoT and blockchain to ensure cyber safety*. Cyber security, once a mere afterthought, now intertwines with the very fabric of our everyday lives.

In addition, and more than ever before, the mantra of "adapt or perish" resonates, propelling businesses to embrace innovation and forge strategic alliances to leave an indelible mark on the ever-evolving business world. This world has become increasingly environmentally conscious as well, and businesses are quick to capitalize on the growing demand for sustainability. However, amidst the hustle for eco-friendly practices, the trend of greenwashing has emerged. Collin W. Keeney looks at this trend in more detail in *Too green to be true: When a well-intentioned statement creates a world of risk*.

And finally, COP 28 is just around the corner, and all eyes are on the region for a direction forward to address the global climate agenda. In *With COP 28 on the horizon, the time to act in the Middle East is now...* by Daniel Gribbin, we see clearly that change is coming and the need to adapt and transition to a low carbon economy is inevitable.

In this world where swift moves dictate our trajectory, it is our responsibility in the end to nurture the positive aspects while navigating the darker corners.

We hope you enjoy this latest Summer issue of the Middle East Point of View.

The ME PoV editorial team

Contents



06

The thriving e-commerce landscape in the Middle East

Dr. Ahmed Hezzah

32

**Too green to be true:
When a well-intentioned
statement creates a world
of risk**

Collin W. Keeney



12

With COP 28 on the horizon, the time to act in the Middle East is now...

Daniel Gribbin

16

On high alert: The darker side of generative AI

Ralph Stobwasser and Nicki Koller

22

The evolving role of finance post IPOs: Shaping the future of finance and the UAE capital markets

Farhad Aklas and Nav Dulay

26

Integrating IoT and blockchain to ensure cyber safety

Govinda Mengji

36

Is artificial intelligence the new benchmark for financial crime risk management?

Humaid Hussain and Khushnood Khan

The thriving e-commerce landscape in the Middle East



Over the past decade, the Middle East has witnessed significant growth in e-commerce, transforming the retail landscape across the region. With advancements in technology, changing consumer behavior, and increased internet penetration, e-commerce has emerged as a key driver of economic growth.

This article explores the rise and impact of e-commerce in the Middle East, encompassing various countries. But first, let's zoom out and examine e-commerce as a worldwide phenomenon.

From brick-and-mortar to click-and-order

Globally, e-commerce has experienced remarkable growth, with online sales surpassing traditional retail channels. In fact, the global e-commerce market is projected to reach a revenue of US\$6.35 trillion by 2027,¹ driven by the ever-growing number of e-commerce users and their reliance on digital platforms for shopping. Factors such as the proliferation of smartphones, improved internet connectivity, and the convenience of online shopping have vastly contributed to this growth.

The COVID-19 pandemic accelerated the adoption of e-commerce worldwide. With lockdowns and social distancing measures in place, consumers turned to online shopping as a safer and more convenient alternative. The pandemic acted as a catalyst for e-commerce growth, particularly in the Middle East where traditional retail had been the dominant mode of commerce.

A new player in the region

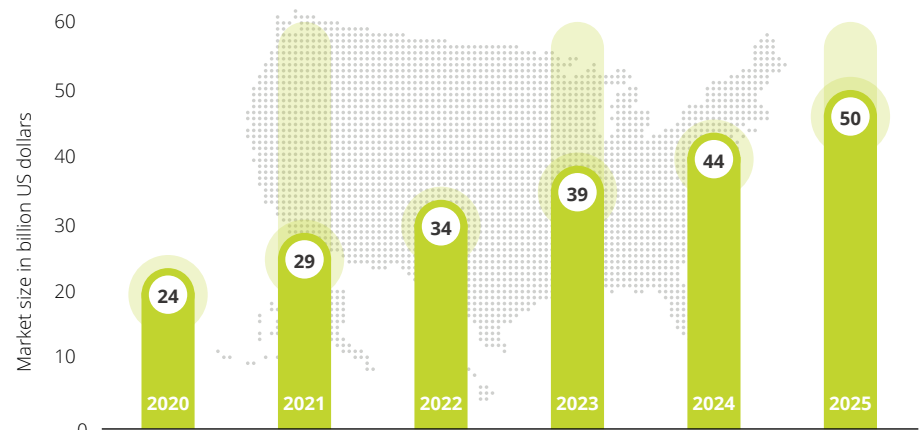
Before the pandemic, e-commerce in the Middle East was still in its nascent stages, but with great room for expansion. The region faced challenges such as limited payment options, lack of trust in online retailers, and a preference for in-store shopping. However, there were notable improvements in internet infrastructure,

smartphone penetration, and the establishment of digital payment systems. A notable shift in consumer behavior across the Middle East was triggered by the unprecedented global health crisis of COVID-19. With restrictions in place, consumers turned to e-commerce platforms for their shopping needs. The demand for essential goods, groceries, electronics, and home products surged. Consumers developed a preference for contactless transactions, leading to an escalating adoption of online payments.

It gradually became apparent that e-commerce has had a profound impact on the Middle Eastern economy and consumer habits. It has provided consumers with convenience, expanded product choices, and competitive prices. E-commerce has also created entrepreneurial opportunities, particularly for small and medium-sized enterprises (SMEs) and individual sellers, leading to job creation and economic empowerment.

The e-commerce sector in the Middle East is poised for substantial growth. It is estimated to reach a market volume of US\$50 billion by 2025,² driven by the widespread use of cutting-edge technologies, and favorable government initiatives to promote digital economies. The region's young and tech-savvy population, coupled with rising disposable incomes, presents a vast consumer base for e-commerce expansion.

With advancements in technology, changing consumer behavior, and increased internet penetration, e-commerce has emerged as a key driver of economic growth



Forecasted e-commerce market size post COVID-19 in the Gulf Cooperation Council region from 2020 to 2025³

E-commerce, e-commerce everywhere!

The evolution of e-commerce has definitely disrupted the traditional retail sector in the Middle East. Brick-and-mortar stores face tough competition from online platforms, leading to a transformation in consumer shopping patterns. Retailers are progressively adapting by establishing their online presence, offering omnichannel experiences, and leveraging technology to enhance the customer journey.

The Middle East e-commerce market encompasses a diverse range of product categories. Fashion and beauty products have seen substantial growth, driven by the region's fashion-conscious population. Online marketplaces and dedicated fashion websites have emerged, catering to the demand for trendy clothing, accessories, and cosmetics. Additionally, the electronics and home appliances sector enjoys a significant market share, fueled by high smartphone adoption rates and the Middle East's tech-savvy consumers. The demand for groceries, health and wellness products, and online food delivery services has also witnessed a noteworthy surge, further bolstering the e-commerce landscape.

Unbounded support

Technological advancements play a crucial role in shaping the e-commerce landscape in the Middle East. One notable trend is the increasing use of artificial intelligence (AI) and machine learning (ML) to personalize the shopping experience, improve product recommendations, and boost customer service. Additionally, the rise of social commerce, influencer marketing, and virtual reality (VR) shopping experiences have transformed how consumers engage with online platforms.

Governments in the Middle East have recognized the potential of e-commerce and have taken various initiatives to further expand its growth. Investment in digital infrastructure, regulations supporting online businesses, and the promotion of digital literacy have been key focus areas. Governments have also established

dedicated e-commerce zones, offering incentives for businesses to establish their operations, and fostering an ecosystem that supports innovation and internship.

Trends and innovations

Alongside the rapid growth of e-commerce in the Middle East, several notable trends have emerged, shaping the industry's trajectory. One such trend is the rise of mobile commerce or m-commerce. With a high use of smartphones in the region, consumers are increasingly using their mobile devices to browse, shop, and make purchases. Retailers have responded by optimizing their websites and apps for mobile devices, and leveraging mobile payment solutions to elevate the shopping experience.

Another trend is the expanding popularity of cross-border e-commerce. Consumers in the Middle East are exploring international online platforms to access a wider range of products, especially those that may be unavailable or harder to find locally. This trend has prompted e-commerce retailers to expand their global reach, offering shipping options and localized experiences to cater to the growing demand. ➤

Governments in the Middle East have recognized the potential of e-commerce and have taken various initiatives to further expand its growth

Personalization and customer experience have become crucial aspects of e-commerce in the Middle East. Online retailers are employing data analytics and customer segmentation strategies to deliver personalized product recommendations, targeted promotions, and tailored shopping experiences. This focus on personalization aims to improve customer satisfaction, increase customer loyalty, and drive repeat purchases.

Furthermore, sustainability and eco-consciousness are gaining traction in the Middle East e-commerce landscape. Consumers are becoming more and more mindful of the environmental impact of their purchasing decisions. E-commerce platforms are responding by promoting sustainable practices such as eco-friendly packaging, carbon offset programs, and offering products from sustainable and ethical brands. This trend aligns with the global shift toward responsible consumption, and presents an opportunity for e-commerce retailers to cater to the evolving values and preferences of Middle Eastern consumers.

The region is also witnessing the rise of social commerce, which combines e-commerce with social media platforms. Social media channels have become influential marketing and sales channels, with consumers discovering products, engaging with brands, and making purchases directly through these platforms. E-commerce retailers are leveraging social media influencers, interactive content, and seamless integration with online stores to drive engagement and conversion.

The future is... bright?

While the Middle East e-commerce market shows tremendous potential, it also faces certain challenges that need to be addressed for sustained growth. One major challenge is the need to build trust and enhance cybersecurity measures. Online fraud and data breaches pose risks to consumer trust in e-commerce platforms.

While the Middle East e-commerce market shows tremendous potential, it also faces certain challenges that need to be addressed for sustained growth. One major challenge is the need to build trust and enhance cybersecurity measures.

Governments, industry players, and consumers themselves need to collaborate to establish robust security protocols and ensure a safe online environment.

Logistics and last-mile delivery infrastructure also pose challenges in the region. With a vast geographic expanse, and varying levels of infrastructure development, ensuring timely and reliable delivery of products can be a complex task. Investments in logistics infrastructure, fulfillment centers, and innovative delivery solutions are essential to address these challenges, and optimize the e-commerce supply chain.

Looking ahead, the future of e-commerce in the Middle East appears promising. The ongoing digital transformation, combined with favorable demographics and sizable disposable incomes, provides fertile ground for e-commerce growth. As more businesses and consumers embrace digital technologies, the e-commerce ecosystem will continue to evolve and mature, driving innovation, job creation, and economic development in the region.

Wrapping up

With the rise of e-commerce, the Middle East has experienced a transformative shift in consumer behavior, retail dynamics, and economic landscapes. The region's vibrant e-commerce market has grown exponentially, driven by factors such as technological progress, changing consumer preferences, and the impact of the COVID-19 pandemic.

While challenges remain, such as building trust, improving logistics infrastructure, and ensuring cybersecurity, the Middle East's e-commerce sector holds immense potential for continued development and innovation. As the region embraces digital transformation, e-commerce will play a pivotal role in shaping the future of retail, trade, and entrepreneurship in the Middle East. ●

By **Dr. Ahmed Hezzah**, Director Consumer and Commerce, Consulting, Deloitte Middle East

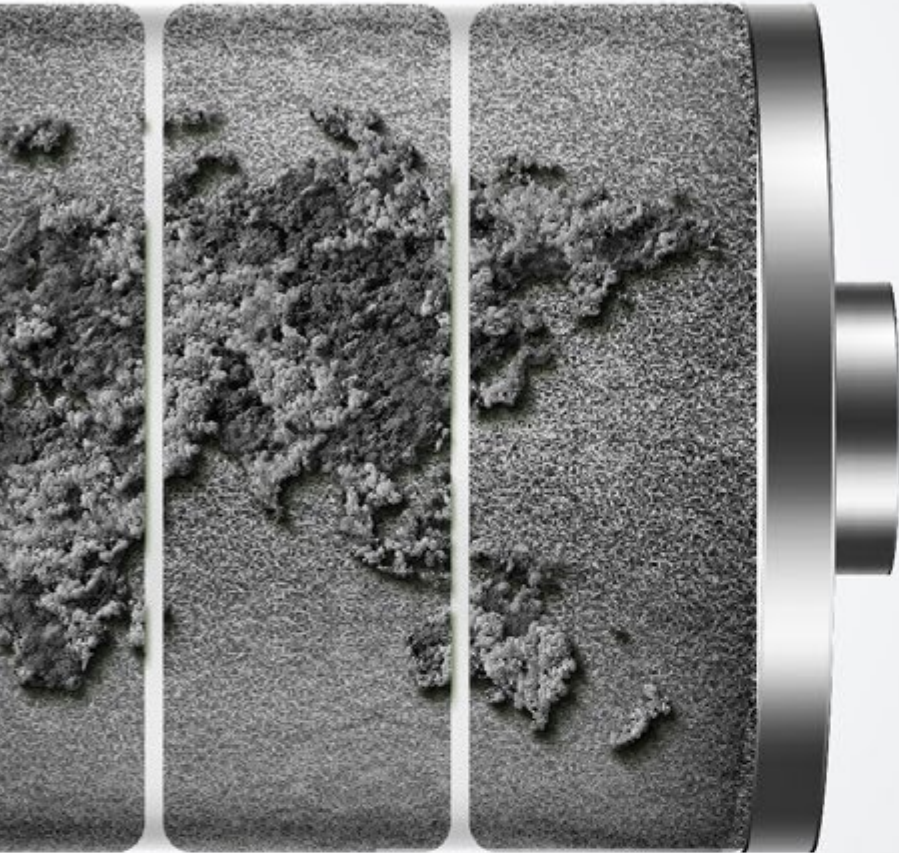
As more businesses and consumers embrace digital technologies, the e-commerce ecosystem will continue to evolve and mature, driving innovation, job creation, and economic development in the region

Endnotes

1. <https://www.statista.com/outlook/dmo/e-commerce/worldwide>.
2. <https://www.statista.com/statistics/1201946/gcc-forecasted-e-commerce-market-size-covid-19/>.
3. <https://www.statista.com/statistics/1201946/gcc-forecasted-e-commerce-market-size-covid-19/>.



**With COP 28 on
the horizon, the
time to act in
the Middle East
is now...**



COP 28 is at the door ... and all eyes are on the biggest hydrocarbon producing region for a pathway forward to explore how to address the emissions crisis. The Middle East has committed to several net-zero related pledges. From Bahrain and the UAE to KSA and Oman, the region has realized that a change is coming for how these historically high petrochemical economies need to adapt and transition to a low carbon economy. But the change is not easy; there are many hurdles that need to be navigated, and many holes that need to be plugged, to allow the region and the world to plan for the next 20-30 years with a lower fossil fuel budget.

COP 27 taught us many things, the least of which is that committing to net-zero is easy, but the hard part is action and meaningful outcomes. A report was produced by the High Level Expert Group on the NetZero Emissions Commitments of Non-State Entities ("Expert Group") which was tasked by the United Nations Secretary General with addressing net-zero pledges and commitments from non state actors including corporations, financial institutions, as well as local and regional

governments. The report outlines ten pledges for the transition, three of which I would like to highlight as crucial to the Middle East, as they require regulatory updates to drive the transition, and above all, transparency and accountability.

In the Middle East, this new regulatory landscape is essential to form the foundation of the low carbon transition plan. There is a need for private and public entities to collaborate in frameworks such as the Race To Zero and the One Planet Sovereign Wealth Fund Framework to ensure everyone's commitment towards the future we all seek. To ensure a positive output, regulators need a full range of fiscal, market, and regulatory mechanisms, including the use of carbon pricing and non pricing mechanisms and incentives, to drive action across the whole ESG landscape. Mechanisms similar to that which we have seen in Europe such as the EU Taxonomy are key to preventing greenwashing. They will help scale up sustainable investments and combat the greenwashing of sustainable financial products and the defining of investments that are qualified as sustainable.

To ensure a positive output, regulators need a full range of fiscal, market, and regulatory mechanisms, including the use of carbon pricing and non pricing mechanisms and incentives, to drive action across the whole ESG landscape

Moreover, the need to create, manage, and disclose transition plans for life after fossil fuels will bring credibility and the alignment among stakeholders. Entities need to create future plans and adjust corporate strategies not just for the next 3-5 years but for 15–20 years. These plans need to be supported by achievable and measurable decarbonization pathways and education across the value chain in order to result in real change. A key element within this, not just in the Middle East but on a global level, will be ensuring that these pathways are fair and achievable. Using credible frameworks such as the Science Based Targets Initiative will give an air of trustworthiness to the commitment of these entities which not only need to be held accountable by the board, but also by the public at large.

Finally, there's a pressing need to disclose progress in an open and transparent manner to ensure accountability. Full data sets and disclosures across the various elements of the ESG spectrum need to be made available and independently validated. The key word to use is that this is a "transition," and entities should not be afraid of reporting or disclosing aspects that they may have fallen short in or need to correct. Stakeholders understand and trust entities that acknowledge both their strengths and their weaknesses, as long as they are in parallel with the sincere commitment to correct the mistakes that might have led to them not achieving their goals in the first place. ●

By **Daniel Gribbin**, Director, Head of ESG Advisory, Deloitte Middle East

Entities need to create future plans and adjust corporate strategies not just for the next 3-5 years but for 15–20 years. These plans need to be supported by achievable and measurable decarbonization pathways and education across the value chain in order to result in real change.

On high alert: The darker side of generative AI





The emergence of new technologies is making our daily lives more convenient, but with the rise of generative AI, to date most notably ChatGPT and DALL-E/DALL-E 2, it has become easier for individuals and organizations to misuse these technologies for malicious purposes. While it is imperative to continue to develop and adopt new technologies, we must also remain vigilant and aware of the potential risks, and take necessary measures to prevent financial crimes, as well as crime on all fronts.

“What is ChatGPT?”

“I am ChatGPT, a large language model trained by OpenAI, based on the GPT (Generative Pre-trained Transformer) architecture. I have been trained on a massive corpus of text data using unsupervised learning techniques to generate natural language responses to a wide variety of prompts and questions. My training data comes from diverse sources, including books, articles, and web pages, allowing me to have a broad knowledge base on a wide range of topics. I can answer questions, generate text, summarize documents, translate languages, and even write stories, among other tasks.”¹

ChatGPT, an example of generative AI, released to the public in November 2022 is software which mimics human language.² Since its launch, it has been at the center of many discussions both in coffee shops and boardrooms. Hailed as a game-changer that makes many tasks easier, such as contract drafting, story writing, and researching, there is potential danger lurking behind the exciting façade. Like any technology, it can unfortunately be misused for criminal purposes. The ease of access to AI and machine learning technology makes it possible for both individuals and organizations to exploit these tools for a wide range of nefarious activities, as both Europol and the UK’s National Cyber Security Centre have recently warned.³

Both advantages and disadvantages stem from the use of generative AI by criminals and for crime prevention. This article will discuss how this tool can enable malicious actors to carry out a range of activities, from fraud and cyberstalking, to impersonation and dissemination of false information.

Firstly, let’s discuss some of the benefits associated with the utilization of generative AI.

While it is imperative to continue to develop and adopt new technologies, we must also remain vigilant and aware of the potential risks, and take necessary measures to prevent financial crimes, as well as crime on all fronts

1. **Crime prevention:** Generative AI can be used to analyze data, and identify patterns in historic data to predict crimes before they happen. For example, it can assist in monitoring social media platforms and online forums for any red flags which may indicate suspicious behavior. This can enable quick and efficient detection, and prevent any potential criminal activity.
2. **Investigative assistance:** Generative AI can be used to analyze large volumes of data, and provide insights that could be difficult for humans to identify. Data from social media platforms may have been traditionally difficult to monitor on an ongoing basis. However, with the processing power of generative AI, this can be monitored quickly and easily to identify potential suspects, predict their movements and activities, and gather evidence to support investigations.
3. **Language translation:** Generative AI can translate different languages, which can be useful when investigators speak a different language to that which they are investigating in. Generative AI can help overcome language barriers in order to shed light on information in different languages, and ensure that investigations are conducted effectively.
4. **Crime analysis:** Similar to crime prediction, generative AI can also be used to analyze data, and identify patterns in historic data to understand crime more effectively. This can help to allocate investigators or enforcement agency resources efficiently, and develop strategies to prevent crime. For example, if a particular area is experiencing a high rate of financial crimes, generative AI can help identify the most common methods used by malicious actors, and provide insights on how to prevent them.

As with any form of artificial intelligence, generative AI has no consciousness; it can't rationalize why it generates the output it produces, and has no real understanding of the human experience. It is purely taught

to behave in a certain way through natural language processing. While limitations have been built into generative AI to mitigate the risk of it being used for nefarious activities, these limitations can be circumvented at times.⁴

Phishing is the most common type of cybercrime attack which, according to a report by Proofpoint, accounted for around 70% of data breaches in 2022

Some of the areas for potential misuse of large language models and AI chatbots include:

Phishing

Phishing is the most common type of cybercrime attack which, according to a report by Proofpoint, accounted for around 70% of data breaches in 2022. It is estimated that 3.4 billion phishing emails are sent every day.⁵ It is no surprise then that it is also one of the most common fraudulent uses of generative AI. Phishing is the process whereby malicious actors send messages, emails, or text messages that appear to derive from a legitimate source, such as a bank, and trick the recipient/victim into providing sensitive information, such as login credentials or financial information. Historically, phishing attacks could be detected through the grammatical and spelling errors within the text. Given generative AI's ability to generate human-like speech, it can be used by malicious actors to mimic the appearance and language use of legitimate sources. The speed and ease with which AI language models, such as generative AI, can be programmed to generate text messages that mimic human communication makes it a powerful tool. It also makes it harder for recipients to detect fictitious and fraudulent emails. >

Malicious actors can use generative AI to create convincing text messages, emails, or other types of content which mimic real people, and ultimately obtain the sensitive information they need

Cybercrime and hacking

Not only does generative AI have natural language processing capabilities, but it can also generate code in various programming languages such as Python, Java, JavaScript, C++, HTML, and CSS. Although the code that is generated may not be optimized for production use, it serves as a starting point. This becomes particularly useful for malicious actors with limited technical knowledge to gain insights to attack a system. It also accelerates the process by which they can optimize their coding to break into systems and the ability for them to translate natural language into working code. To extend on this, generative AI has also seen the ability to flow between programming languages and natural languages, making it easier for such malicious actors to build “end to end” malicious campaigns, which may start with phishing attempts, and end in the generation of malicious software.⁶

Impersonation

As digital identity verification becomes more common place, the risk of fraudulent identities and impersonation increases. The Guardian heralds ChatGPT as the best software program for impersonating humans ever released to the public.⁷ The danger is that this can be used for fraudulent means, including the use of fake identities to access sensitive information, and stealing funds through unauthorized financial transactions. Malicious actors can use generative AI to create convincing text messages, emails, or other types of content which mimic real people, and ultimately obtain the sensitive information they need. Additionally, tools such as DALL-E can be used as a kind of natural language Photoshop to create convincing yet fake photos.⁸

Impersonation can cause significant damage to the impersonated individual

and company, both reputational and financial. The ease with which generative AI can generate convincing text messages, coupled with the natural feel of the generated output, makes it a powerful tool overall.

Dissemination of false information/propaganda

The dissemination of false information and propaganda is a growing concern in the digital age. Generative AI can be used to create false and convincing content, including social media posts and other types of content that are designed to mislead and deceive individuals. Additionally, generative AI can be used to generate and disseminate fake news at an increased speed and volume, which can have a detrimental impact on society, as we have seen time and again. This shows the use case in terrorism and propaganda as well. NewsGuard performed an exercise whereby they prompted ChatGPT on 100 false narratives. Although there are limitations which exist to prevent the generation of fake information, they achieved incorrect but articulate and fluent claims regarding 80% of the topics shared with ChatGPT to prompt fake news.⁹ Generative AI can generate legitimate looking text messages that appear to be written by a human, as well as fake photos which can appear to be compromising for an individual; this makes it difficult for individuals to detect that they contain false information. The ease with which generative AI can be programmed to generate false information makes it a powerful tool for those who seek to deceive and mislead.

There is no doubt that ChatGPT and DALL-E have not only brought the topic of generative AI to the forefront of the public, but also have become a commonplace tool for many. Coupled with its benefits,

generative AI's criminal use is a real concern. In all the above cases, we can see how the speed, ease, and ability to mimic humans can pose a risk for fraudulent behavior against individuals and organizations.

To mitigate the risks of generative AI, individuals and organizations should drive awareness of these risks alongside the benefits. There is no doubt that generative AI and other AI-based tools can support law enforcement and regulators with detecting fraudulent behavior, preventing crime, supporting investigations, and analyzing crime data. As Sam Altman, the CEO for OpenAI, stated in a US Senate hearing, "We think that regulatory intervention by governments will be critical to mitigate the risks of increasingly powerful models."¹⁰ It's vital to ensure that these tools are used responsibly and measures are put in place to prevent their misuse for criminal activities. ●

By **Ralph Stobwasser**, Partner, Forensic and **Nicki Koller**, Manager, Forensic, Deloitte Middle East

Endnotes

1. <https://chat.openai.com/>.
2. <https://openaimaster.com/chat-gpt-login/>.
3. <https://www.ncsc.gov.uk/blog-post/chatgpt-and-large-language-models-whats-the-risk>; <https://www.europol.europa.eu/media-press/newsroom/news/criminal-use-of-chatgpt-cautionary-tale-about-large-language-models>.
4. <https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf>.
5. <https://aag-it.com/the-latest-phishing-statistics/#:~:text=The%20US%2Dbased%20IC3%20received,than%20%242.7%20billion%20in%202022>.
6. <https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf>.
7. <https://www.theguardian.com/commentisfree/2022/dec/08/the-guardian-view-on-chatgpt-an-eerily-good-human-impersonator>.
8. <https://www.techtarget.com/searchenterpriseai/feature/A-closer-look-at-what-makes-the-AI-tool-Dall-E-powerful>.
9. <https://www.newsguardtech.com/misinformation-monitor/jan-2023/>.
10. <https://www.theguardian.com/technology/2023/may/16/ceo-openai-chatgpt-ai-tech-regulations>.

There is no doubt that generative AI and other AI based tools can support law enforcement and regulators with detecting fraudulent behavior, preventing crime, supporting investigations, and analyzing crime data

The evolving role of finance post IPOs: Shaping the future of finance and the UAE capital markets



The United Arab Emirates (UAE) has continued to experience strong economic growth despite the recent global headwinds, as a result of continued economic diversification and government investment which further positions the country as a global economic powerhouse. With increased investment in sectors such as tourism, logistics, real estate, financial services, and technology, the country's commitment to innovation and entrepreneurship has positioned it as a regional leader for leading businesses – both private and public.

Given the dynamics of the economic landscape, the UAE has emerged as a prominent destination for initial public offerings (IPOs), which reflects the country's commitment to foster a robust capital market and attract global investment.

In recent years, there has been a notable increase in IPOs across various sectors. This surge has been attributed to various factors including the government's emphasis on economic diversification, political stability, financial regulatory reform, and the UAE's strategic location and position as a global business hub, as a result of which the number of entities listed on the two primary stock exchanges in the UAE, Dubai Financial Market (DFM) and Abu Dhabi Stock Exchange (ADX), has increased by approximately 10% over a period of 12 months.¹ These IPOs have attracted significant interest from both retail and institutional investors resulting in multifold oversubscription, and reflecting the region's growing investor appetite for emerging growth opportunities.

Key considerations for the finance function

In recent years, the role of the finance function of a listed company in IPOs has undergone significant changes, driven by evolving market dynamics, technological advancements, and shifting investor preferences, with increased importance on the role of finance from strategic financial planning to ESG considerations and communication. While organizations spend considerable time and resources identifying and addressing potential anticipated changes as part of their IPO readiness, many within the finance function have found their roles significantly change post listing.

Given the changing landscape, and having worked with a number of organizations pre and post IPO, here are five key considerations (non-exhaustive) that finance professionals and those charged with governance need to consider post an IPO:

1. Accelerated financial reporting timelines

Listed companies in the UAE must adhere to stringent reporting timelines outlined by the Securities and Commodities Authority (SCA). SCA requirements mandate that companies disclose their quarterly earnings within 45 days following the end of the reporting period, while audited financial statements must be issued within 90 days from the end of the financial year. There are also additional International Financial Reporting Standard (IFRS) disclosures required for entities with publicly traded securities. The finance functions of these

companies should consider the scheduled dates for audit committee and board approvals, allowing sufficient time to address any feedback or queries raised by these committees prior to reporting. Although some organizations may have existing internal reporting timeframes prior to listing, allowing for slight flexibility with a few days' delay which diminishes post-listing. Any delay in meeting the reporting deadlines can result in a suspension of share trading and damage to the company's reputation.

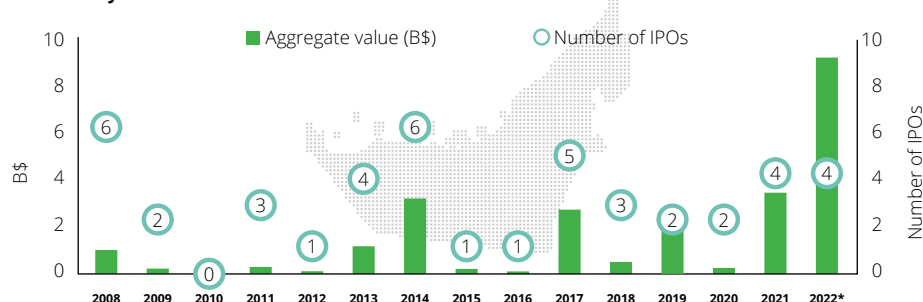
2. Enhanced investor communication and the role of finance

Effectively communicating results to investors and analysts is vital for a publicly traded company, with significant dates like quarterly earnings calls being essential for any listed company. While the finance team in a private company primarily focuses on internal reporting and analysis, this changes post listing. After going public, the finance team is required to collaborate closely with the investor relations team to deliver coherent financial narratives to the market. The ability to convey quarterly results and trends clearly and succinctly is critical for establishing investor confidence, attracting capital, and improving financial transparency. Furthermore, a capable finance team can anticipate potential inquiries, gather the necessary information, and effectively relay it to the investor relations team, enabling the CFO/CEO to address those inquiries.

3. A change in auditor rotation requirements

The UAE requires all listed companies to rotate their auditors in line with the SCA rotation rule, which mandates audit engagement partner rotation every three years and for the audit firm to be rotated every six years. These rules were enforced to bolster transparency and accountability, along with promoting independence and objectivity. Finance teams, who may lack prior experience with audit transitions, must swiftly adapt to a different audit approach. They must also establish relationships with the new audit firm and consider the additional time needed for

IPO activity in the UAE since 2008



Data compiled 16 June 2022. Analysis includes initial public offerings covered by S&P Global Market Intelligence completed since 2008. Terminated/withdrawn IPOs have been excluded from the sample. *Data as of 16 June 2022. Source: S&P Global Market Intelligence

the new auditor to familiarize themselves with previous complex and judgmental accounting matters.

4. Increased governance responsibilities

Those responsible for governance have the duty to oversee a company's financial reporting process. As a company transitions from being private to going public, the significance of robust corporate governance increases significantly to inspire confidence in investors and shareholders. One of the primary responsibilities of the audit committee in a listed company is to ensure adherence to the auditor independence rule, guaranteeing that any non-audit services provided by the auditor do not compromise their independence. Listed companies, classified as 'public interest entities,' are subject to stricter independence regulations, with recent amendments to the International Ethics Standards Board for Accountants (IESBA) International Code of Ethics for Professional Accountants (including International Independence Standards) introducing additional safeguards that governance must be aware of. The mandated 6-year auditor rotation rule introduces further complexities, necessitating monitoring of non-audit services provided by other audit firms to ensure that preferred bidders during rotation remain eligible and free from conflicts of interest.

5. Internal controls over financial reporting

Finance teams will need to update their internal control systems to ensure compliance with additional regulatory requirements that follow a listing. As outlined in the article "Keeping up with internal controls" in the ME PoV Winter 2022 issue, the SCA issued a revised draft Governance Code for public consultation in the UAE in September 2022, which indicated that the auditor's responsibilities will be enhanced to include an opinion on the effectiveness of ICFR for all listed entities in the UAE. Companies that were not previously subject to an ICFR audit will need to assess their readiness for such an

audit and the finance team will play a key role in this process.

With the UAE positioned as the hub for innovation, the IPO market is poised for continued expansion. The increased momentum will continue to attract both local and global companies seeking to capitalize on the UAE's dynamic and investor friendly ecosystem, which will further support the government's ambition to fortify the country's reputation globally.

In response, finance teams are increasingly being asked to be more strategic, digital and investor focused, coupled with considering areas such as ESG. Talent acquisition and development within the finance function are vital components in supporting a successful IPO and in creating a robust finance framework post IPO to ensure financial reporting compliance. This requires skilled and experienced finance teams that can navigate the complexities of the process. Equipping current finance teams and developing their skills is essential to ensure that they have the necessary skills and knowledge required for post IPO success. ●

By **Farhad Aklas**, Partner, Audit & Assurance and **Nav Dulay**, Director, Audit & Assurance, Deloitte Middle East

In recent years, the role of the finance function of a listed company in IPOs has undergone significant changes, driven by evolving market dynamics, technological advancements, and shifting investor preferences, with increased importance on the role of finance from strategic financial planning to ESG considerations and communication

Endnotes

1. S&P Global Market Intelligence – IPO activity in the UAE since 2008 - <https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/competition-heats-up-as-banks-try-to-cash-in-on-uae-s-ipo-boom-70784270>.

Integrating IoT and blockchain to ensure cyber safety



IoT and blockchain have become buzzwords in the current technological era, a time when technology can help to solve problems, yet also generate new challenges. Cybersecurity is one such major challenge that is hindering the fearless usage of technology. The solution lies in how effectively these technologies are integrated and implemented. Hence, this article is an overview of the integration of IoT and blockchain to ensure cyber safety. It also discusses the essential security measures, and lists the IoT security challenges.

An IoT overview

The network of physical electronic devices, machines, and other objects, which are implanted with sensors and software for the purpose of communicating and exchanging data with other devices and systems through the internet, and each of which has an IP address, is referred to as the Internet of Things (IoT). Today, IoT plays a major role in transforming our lives, and as technologies are enhancing, hackers and cybercriminals are developing new, high-tech ways to breach secure and private data. However, with significant advancement in the IoT range, the issues related to data and information security need to be addressed.

The IoT has enormous advantages, however, it often lacks security. Ideally, user data must be kept private and safe. For this reason, better security measures must be created, maintained, and made the norm for IoT and linked devices in order to keep data secure. In addition, the IoT makes it possible to share data and information via blockchain.

Some of the major IoT security challenges include:

- Visibility and transference
- Data privacy, confidentiality, and integrity
- Authentication, authorization, and accounting
- Secure communications
- Data encryption
- Middleware security

A blockchain overview

Blockchain is an indispensable technology that has been hitting the headlines due to the popularity of cryptocurrencies such as Bitcoin and Ethereum. Is blockchain only concerned with cryptocurrencies? The answer is an emphatic no. Blockchain technology has moved beyond cryptocurrencies to another level. Blockchain is a distributed, decentralized, immutable ledger that can be used to record transactions and track assets in a business network; with blockchain, the intermediary in digital transactions is eliminated. So simply put, in a blockchain, each block in the chain represents a record, and the chain links all of the blocks together.

Key security features of blockchain:

- **Cryptographic security:** Hash functions are one-way functions where it is simple to go ahead (from input to output) but computationally impossible to move backward (output to input).
- **Identity management:** Blockchain identity management systems address current identity issues such as inaccessibility, data insecurity, and fraudulent identities.
- **Multisignature:** Blockchains use digital signatures to ensure the authenticity and integrity of transactions; multisignature requires multiple private keys to generate a valid digital signature, allowing multiple parties to approve a transaction. Furthermore, in blockchain technology, it is infeasible to break public key cryptography, even by brute force guessing.
- **Data privacy:** As data in blockchain is immutable, and blockchain networks can be configured in private/public or permissioned/open blockchains, it offers the potential for enhanced data privacy and control. In a blockchain, data is stored in a decentralized and distributed manner across multiple nodes. Each transaction of data added to the blockchain networks is cryptographically hashed and linked to the previous block, creating an immutable and transparent ledger.

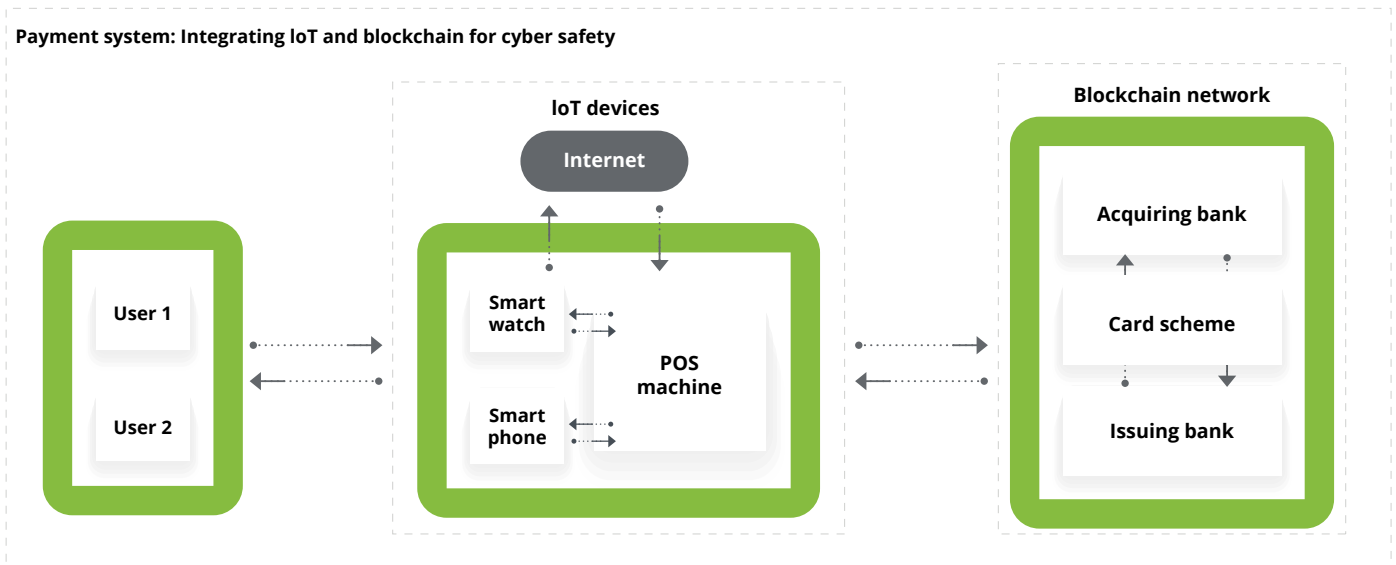
- **Secure communication:** Blockchain can ensure that an attacker cannot monitor and change the communications occurring between nodes, thus maintaining the integrity and confidentiality of the network.

IoT and blockchain are both fantastic innovations on their own, but when they are combined and implemented, they can generate astounding outcomes that are beneficial for cyber safety.

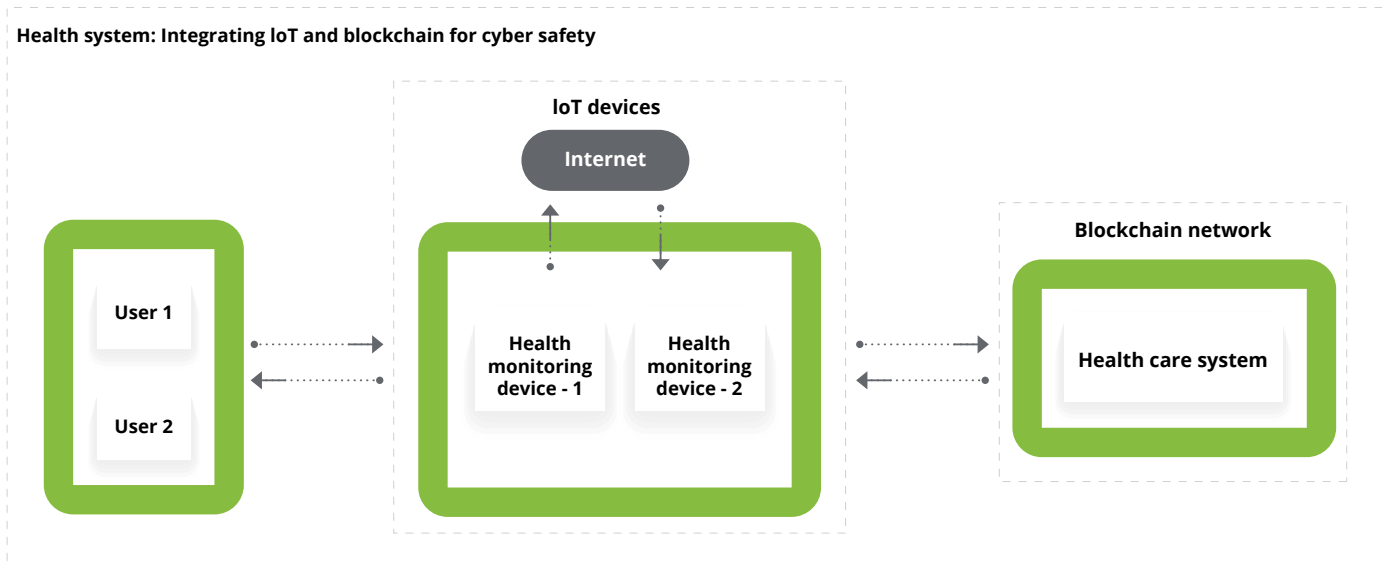
Below are the use cases on integrating IoT and blockchain to ensure cyber safety: ➤

Blockchain is a distributed, decentralized, immutable ledger that can be used to record transactions and track assets in a business network; with blockchain, the intermediary in digital transactions is eliminated

Use case A:



Use case B:



Currently, IoT technology is used with conventional databases. In the high-level block diagrams (Use case A and Use case B) the payment and health care systems can be replaced by blockchain technology. However, the process and flow remain the same.

By adopting blockchain technology, it is possible to address the following IoT cyber security concerns:

- Blockchain is based on the peer-to-peer network in which all nodes have the same copy of records, which solves data integrity issues.
- Blockchain can be implemented in private/public permissioned/open blockchains. It ensures access control, and prevents unauthorized access for data privacy. Furthermore, blockchain can keep track of data gathered by sensors, and prevent fraudsters from duplicating it with other harmful types of data.
- ECDSA (Elliptic Curve Digital Signature Algorithm) solves the limitation of IPV6 address.
- Blockchain network can track every transaction and record, which addresses the problems with trusted accountability.
- Blockchain network will be connected to multiple nodes; it will be resilient and fault tolerant, which solves the problem of single points of failure.
- Blockchain hashing function generates a unique ID that can be assigned to each IoT device. Furthermore, each transaction/record will be tracked in the blockchain network, which will solve the problem of identifying the trusted origin of data.
- Blockchain operates on read and write operations only; data in blockchain is immutable, which will address the data compromise and data manipulation issues.

IoT and blockchain are both fantastic innovations on their own, but when they are combined and implemented, they can generate astounding outcomes that are beneficial for cyber safety

- Blockchain technology is third party risk free, as it can perform operations without the intermediary or third party.
- Smart contract programs help to develop access rights and customize the policies based on the requirements.

The future of the financial sectors and other industries is becoming increasingly digital, which makes the process more convenient for end consumers. Internet of Things (IoT) and blockchain technology are part of this rapid transition towards the bank of the future; both end users and financial sectors, as well as other industries, need to adapt to these trends for cyber safety. Thus, with the development of high-speed networks and sophisticated network devices, IoT is unquestionably an emerging technology. IoT currently faces security limitations and concerns, some of which can be addressed by incorporating blockchain technology. The challenges of technology and cybersecurity are two sides of the same coin. The importance of cyber safety increases as technology evolves. ●

By **Govinda Mengji**, Specialist Master, Risk Advisory, Cyber & Strategic Risk, Blockchain, Cloud, IT-DR, Deloitte Middle East

The future of the financial sectors and other industries is becoming increasingly digital, which makes the process more convenient for end consumers. Internet of Things (IoT) and blockchain technology are part of this rapid transition towards the bank of the future; both end users and financial sectors, as well as other industries, need to adapt to these trends for cyber safety.

Too green to be true: When a well- intentioned statement creates a world of risk





In today's increasingly environmentally conscious world, businesses are quick to capitalize on the growing demand for sustainability. However, amidst the hustle for eco-friendly practices, an unfortunate trend has emerged: greenwashing. As we delve deeper into the complexities of greenwashing, it becomes crucial to navigate this maze of half-truths and identify the true champions of environmental management.

"We will be carbon neutral by 2030."

"This project will be self-sustaining, and fuelled entirely by sustainable sources."

"Our products are 100% ethically sourced."

Statements like these have been the subject of regulatory intervention under anti-greenwashing rules. On one hand, they appear to be earnest statements, demonstrating a company's commitment to sustainability. On the other hand, they could be well-intentioned, but perhaps a bit cavalier or hollow in their aspirational approach. At the extreme, they could pose as simply cynical and even deceitful. These are just a few examples of the types of statements that could be central to greenwashing actions.

An overview

What is greenwashing?

Greenwashing refers to the intentional practice of deceiving, misleading, or confusing consumers and investors by presenting a company, initiative, or product as environmentally or socially friendly, or claiming specific environmental or social benefits or impacts when those claims are in fact questionable.

Why does greenwashing matter?

Greenwashing is significant for several reasons. Environmental, social, and governance (ESG) investing is rapidly growing; indices, rating agencies, investors, and funds are increasingly focusing on ESG-mandated investment strategies. According to Deloitte's projections, by

2024, approximately US\$80 trillion, which represents half of the global assets under professional management, will be ESG-mandated.¹ This shift indicates a strong demand for investments that align with sustainability objectives.

Similarly, consumers and businesses make marketplace decisions that can be influenced by the same social or environmental consciousness. According to a 2023 YouGov survey in the UK, where consumer spending is approaching US\$2 trillion per year, "a majority of consumers take into account environmental (66%) and social factors (70%) when making a purchase decision."² Incidentally, those numbers rise to 78% and 79% respectively for consumers in the UAE.³

Given the substantial amount of investment and consumer capital directed towards sustainable targets, it is increasingly crucial for companies to establish their sustainability credentials. Whether they are seeking investment capital, or aiming to capture consumers' attention, defining themselves in sustainability terms has become imperative. The question then becomes: Are their sustainability-related claims accurate? If these claims are false, are they intentionally and knowingly misleading, intended to deceive consumers or manipulate the markets?

How are allegations likely to surface?

Companies operating in today's globally-integrated markets have a wide range of stakeholders, including consumers, clients, employees, vendors, investors, regulators, governments, civil society organizations, NGOs, and even competitors. These stakeholders can be dispersed across multiple countries, resulting in a diverse and expansive stakeholder landscape. Whistleblowers can emerge from any corner of this complex network of stakeholders.

The nature of greenwashing allegations, and the manner in which they arise, can significantly impact the approach taken during an investigation.

A greenwashing allegation can carry serious consequences. It is subject to formal regulation by securities regulators who seek to protect the accuracy and reliability of market information, the potential threat of civil litigation from environmental groups or NGOs, and informally by the markets and consumers. Several regulators have emphasized that tackling greenwashing is already a priority on their enforcement agenda, with an increasing focus going forward.

It should be noted that for any company with connections to the US, the Dodd-Frank Act and the SEC Whistleblower Program provide incentives for potential whistleblowers to report serious allegations of corporate wrongdoing directly to regulators. If allegations are proven valid, the whistleblowers may be eligible for 15-30% of the fines or sanctions levied by the regulator. It is important for overseas branches and non-US companies to be aware that the reach of US regulators extends globally, and therefore, should not disregard the potential applicability of these regulations to their operations.

This underscores the urgency for companies to have strong internal whistleblowing policies that promote and protect good faith internal reporting. A whistleblower is more likely to go straight to the authorities (regardless of any reward) if they do not feel safe from retaliation or feel that they are not being taken seriously internally.

What happens next? How and what should be investigated?

The answer to this depends on the nature of the allegation. Is it an unsupported statement made to the markets which has attracted scrutiny from regulators or whistleblowers? Alternatively, does it involve deeper issues, such as allegations of cover-ups regarding environmental, social, or governance-related violations that challenge a company's stated ESG agenda? The course of action would vary for each scenario, however, in both cases, two aspects will need to be addressed:

1. Accuracy of the allegation: Is there an issue that needs to be addressed?
2. What is the severity of the issue and who is involved?

Taking the first scenario into consideration, where a company has allegedly made an unsupported ESG-related statement to the markets, there are some aspects to consider:

The intention behind it: Is it a benign, aspirational statement or a commitment to a specific outcome? This can be determined from the statement itself, for example, a general statement on a website such as “our company is committed to a more sustainable and just future” may not carry as much regulatory risk as a fund prospectus making misleading or unsubstantiated claims about the ESG credentials of its investment portfolio.

The substance of the statement: Is it reasonable and supportable? This question is quite complex and requires subject matter expertise in the relevant fields. An independent expert should be instructed to review the substance of the statement from a technical standpoint and try to answer questions around topics such as: Is the statement technically feasible? Has the company conducted relevant studies to support it? Has the company made tangible progress towards that goal? Has it developed key considerations such as regulatory approval, project financing, etc.? Is there a defined program to deliver the stated outcome with timeframes, contingency plans, and risk assessment?

The company's seriousness about ESG:

Does it demonstrate commitment and purpose? This pertains to the overall quality of the ESG program and the compliance apparatus around it. The considerations could be two-fold. Firstly, are the allegations arising despite the company's best efforts to live by its ESG commitments or is it simply a mistake or a bad apple? Secondly, if there is a penalty or fine arising from the violation, the company's ability to demonstrate the quality and rigor of its ESG program could help it reduce penalties.

After considering the aforementioned points, the company will be in a better position to evaluate whether it has a greenwashing issue to be concerned about or not. If so, and the matter has the prospect for regulatory action or civil litigation, there may be a requirement to disclose the matter to the government regulator, depending on the jurisdiction. This can make it essential for the company to establish legal privilege over the investigation, which is typically achieved by instructing external legal counsel to oversee the investigation process. Further investigation should then be conducted to understand the knowledge and intention of the individuals involved, the timeline of associated events, as well as the benefits earned, following an established, robust process similar to other business conduct investigations.

ESG is serious business, and is being taken seriously by investors, society, and increasingly by regulators. As companies embrace the benefits of aligning themselves with the sustainability movement, they need to be cognizant of the risks of letting their words move faster than their actions. ●

By **Collin W. Keeney**, Partner, Forensic, Deloitte Middle East

Endnotes

1. <https://www2.deloitte.com/us/en/insights/industry/financial-services/esg-investing-and-sustainability.html>.
2. <https://business.yougov.com/content/7678-global-market-analysis-esg-importance-consumer-purchase-decisions>.
3. <https://www.macrotrends.net/countries/GBR/united-kingdom/consumer-spending>.

Given the substantial amount of investment and consumer capital directed towards sustainable targets, it is increasingly crucial for companies to establish their sustainability credentials. Whether they are seeking investment capital, or aiming to capture consumers' attention, defining themselves in sustainability terms has become imperative.

Is artificial intelligence the new benchmark for financial crime risk management?





The Middle Eastern financial services industry (FSI) has experienced rapid growth in the post-pandemic era.¹ The initial lockdowns compelled financial institutions (FIs) to enable digital accessibility of their offerings to existing and prospective customers. This digital transformation, enacted in a short duration, led to the creation of risk that financial criminals have exploited.²

In response, FSI regulators in the Gulf Cooperation Council (GCC) have increased their efforts to combat rising financial crime risks. Recently, they have been encouraging market participants to integrate technologies into their respective financial crime control frameworks, issuing regulations and guidance to support FIs to effectively combat financial crime. Such directives include:

- The Central Bank of the United Arab Emirates (CBUAE) issued a guidance note encouraging FIs to use 'Digital ID' systems (referring to technology that uses electronic means to assert and prove a person's identity online and/or in in-person environments) to perform customer due diligence.³
- The Saudi Central Bank (SAMA) issued their 'Counter-Fraud Framework,' where it mandates FIs to define, approve, and implement a strategy for the sourcing/development and implementation of counter-fraud systems and technology to manage their fraud risks.⁴
- In its 'Anti-Money Laundering and Combating Terrorism Financing Instructions,' the Qatar Central Bank (QCB) mandates FIs to maintain sufficient resources, including technology, to effectively mitigate its respective financial crime risk.⁵

This article examines how FIs can integrate suitable anti-financial crime technologies in two key processes: identity verification and transaction monitoring.

Identity verification

The primary financial crime risk that FIs face when onboarding a new customer via their

digital channels is impersonation fraud (i.e., an individual who poses as another to open an account; such accounts can then be used to facilitate criminal activity). FIs currently use controls such as multi-factor authentication (e.g., one-time-passwords, authentications apps) to mitigate the risk. However, financial criminals have found methods to defeat such controls.⁶

Advancements in technology, in the form of artificial intelligence (AI), now provide FIs with more sophisticated solutions that can be adopted to either complement or replace their existing controls that verify the identities of prospective and existing customers. Two such solutions include:

- **Identification document verification solutions:** FIs can integrate a solution that scans the prospective customer's live identification documents when uploaded onto the FI's digital channel via the prospective customer's mobile phone or computer to determine their validity and authenticity. This verification is performed through a variety of checks, such as hologram analysis, security patterns analysis, color analysis, and light and blur detection.
- **Biometric validation solutions:** FIs can integrate an advanced biometric validation solution, which verifies the identity of the prospective customer through numerous checks (e.g., facial recognition, liveness detection, age detection, gender detection, blinking analysis, mood analysis, behaviour analysis). Such tools can be customized in terms of the number of checks based on each FI's level of risk. Additionally, this technology can be leveraged to validate the identity of existing customers as well. For example, when a customer initiates a high-value transaction through a digital channel (i.e., mobile banking, online banking), an advanced biometric validation can be performed as confirmation the actual customer has actioned this.

Through such AI-driven solutions, FIs can significantly mitigate the risk of

manipulation in their digital account opening and other identity verification processes. This technology can be leveraged to optimize financial crime compliance resources (e.g., replacement of one-time password OTP systems, re-purposing of manual reviewers) and provide cost benefits as well.

FSI regulators in the Gulf Cooperation Council (GCC) have increased their efforts to combat rising financial crime risks. Recently, they have been encouraging market participants to integrate technologies into their respective financial crime control frameworks, issuing regulations and guidance to support FIs to effectively combat financial crime.

Transaction Monitoring (TM)

As digital payment volumes surge in the region,⁷ FIs are looking at ways to optimize their TM frameworks. Regulators such as the CBUAE have enabled FIs to explore dynamic intelligence-led TM models, which can enable FIs to identify wider networks in which customers operate instead of only individual transactions.⁸ The current rules-based TM models to TM solutions adopted by FIs are only as effective as the quality of data feeding them.⁹ The following are two AI-driven solutions that can augment the FIs' incumbent TM frameworks and support them in their TM optimization journeys:

- **Transaction analysis solutions:** FIs can integrate transaction analysis solutions, which can assess multiple data points linked to a transaction (e.g., transaction value, channel used, geographies involved, parties involved) to uncover highly complex and unusual patterns that may be linked to previously unknown financial crime schemes. This analysis can, subsequently, drive the TM system fine-tuning process in the form of updated scenarios, rules, and thresholds, and result in fewer false positives.
- **Specialized trade-based TM solutions:** FIs with higher volumes of trade-based business activity can integrate a specialized solution to detect trade-based money laundering. Such solutions can support the FI by automating large parts of the due diligence process (e.g., document extraction, verification, screening alerts, document image processing, document categorization, compliance checks, red flags, consistency check and text reconciliation) and providing additional protection against one of the most common methods of money laundering.

The inclusion of AI in the TM process can be a game-changer. Through proper implementation, manual tasks such as TM alert investigations (e.g., customer profile analysis, narrative development) can be automated, providing FIs time and cost efficiencies without any compromise

on financial crime risk management. The adoption of such technologies will require a hybrid approach in initial phases, where technology performs labor-intensive tasks and humans provide oversight (including final decision-making), until intelligence-led TM models can prove to be more effective.

The use cases for AI-driven solutions are numerous, and their benefits are apparent (i.e., cost efficiencies, comprehensive reviews, time efficiencies, reduced errors, data-backed insights). In line with regulatory strategy across the Middle East, FIs should review their financial crime risk management strategies and consider making technology a focal component in order to realize the true benefits that AI can deliver for business and compliance. ●

By **Khushnood Khan**, Director, Financial Crime & Data Analytics and **Humaid Hussain**, Assistant Manager, Financial Crime & Data Analytics, Deloitte Middle East

Endnotes

1. 'Middle East Banks Witnessing Digital Revolution,' Evalueserve, undated.
2. 'Financial crime risk rises in the Middle East and North Africa,' Refinitiv, 30 June 2021.
3. 'Guidance for Licensed Financial Institutions on Digital Identification for Customer Due Diligence,' CBUAE, 31 October 2022.
4. 'Counter-Fraud Framework,' SAMA, October 2022.
5. 'Anti-Money Laundering and Combating Terrorism Financing Instructions,' QCB, May 2020.
6. 'Scammers Are Cracking Today's More Secure Passwords — Here's What You Can Do,' Forbes, 25 July 2022.
7. 'Rise of Digital Payments in MENA Region: 2023 Digital Payment Trends,' Fintech News, 8 February 2023.
8. 'Guidance for Licensed Financial Institutions on Suspicious Transaction Reporting,' CBUAE, 7 June 2021.
9. 'Transaction Monitoring Optimisation: Using an intelligence lead approach to Transaction Monitoring,' Deloitte, 2022.

In line with regulatory strategy across the Middle East, FIs should review their financial crime risk management strategies and consider making technology a focal component in order to realize the true benefits that AI can deliver for business and compliance

Thought leadership publications from Deloitte

ME PoV provides you with a selection of Deloitte's most recent publications accessible on Deloitte.com

ME PoV

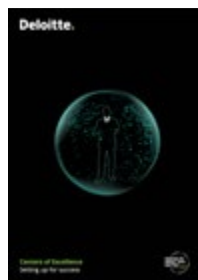
Consulting



ME PoV Spring 2023
The case for diversity and inclusion



Reimagining Finance operations in the digital age



Centers of Excellence - Setting up for success
The race to adopt Excellence is on



S.A.G.E. The Deloitte Framework to establish a leading Higher Education institution in the Kingdom of Saudi Arabia



Deloitte Global Marketing Trends 2023 - Middle East Resilient seeds for growth

Financial Advisory

Tax

Diversity

Climate



Real Estate Predictions 2023
A market overview of Dubai and KSA



Key features of the newly issued Corporate Tax law



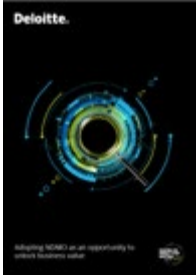
Women @ Work 2023: A Global Outlook



Deloitte 2023 CxO Sustainability Report



Annual global competitiveness overview
Who is winning the race?



Adopting NDMO as an opportunity to unlock business value



Social care for the elderly in the Middle East



ME Human Capital Trends 2023
New fundamentals for a boundaryless world



Technology, Media, and Telecommunications Predictions 2023

TMT

Risk Advisory

Human Capital



Tech Trends 2023



2023 Global Future of Cyber Survey



Impactful board members
Attributes that add value



Board Impact
Understanding and measuring the value of a board

Deloitte offices

Regional office
Gefinor Center, Block D
Clemenceau Street
P.O. Box 113-5144
Beirut, Lebanon
Phone +961 (0) 1 748 444
Fax +961 (0) 1 748 999

Consulting
Emaar Square, Building 1, level 2
Downtown Dubai
P.O. Box 4254
Dubai, United Arab Emirates
Phone +971 (0) 4 376 8888
Fax +971 (0) 4 376 8899

Deloitte Digital Center
Al Ra'idah Digital City
Building: RDC IN 01, 1st floor
Riyadh, Saudi Arabia
Phone +966 (0) 11 404 5900

Financial Advisory
Al Fattan Currency House
Building 1, DIFC
P.O. Box 112865
Dubai, United Arab Emirates
Phone +971 (0) 4 506 4700
Fax +971 (0) 4 327 3637

Risk Advisory
Emaar Square, Building 3, level 6
Downtown Dubai
P.O. Box 4254
Dubai, United Arab Emirates
Phone +971 (0) 4 376 8888
Fax +971 (0) 4 376 8899

Tax & Legal
Al Fattan Currency House
Building 1, DIFC
P.O. Box 282056
Dubai, United Arab Emirates
Phone +971 (0) 4 506 4700
Fax +971 (0) 4 327 3637

Bahrain
Manama
United Tower
Bahrain Bay
P.O. Box 421
Manama, Kingdom of Bahrain
Phone +973 (0) 1 721 4490
Fax +973 (0) 1 721 4550

Cyprus
Nicosia
24 Spyrou Kyprianou Avenue
CY1075
Nicosia, Cyprus
Phone +357 (0) 22 360300
Fax +357 (0) 22 360400

Limassol
Maximos Plaza, Block 1, 3rd floor
213, Arch. Makariou III Avenue
CY3030
Limassol, Cyprus
Phone +357 (0) 25 868686
Fax +357 (0) 25 868600

Egypt
Cairo
Nile City South Tower, 6th floor
2005 A Cornish El Nile
Ramlet Boulq
Cairo, Egypt
Phone +20 (0) 2 246 199 09
Fax +20 (0) 2 246 199 04

Alexandria
Madinet El Sayadla
Building No 10, Smouha
Alexandria, Egypt
Phone +20 (0) 3 426 4975
Fax +20 (0) 3 426 4975

Iraq
Erbil
Empire Business Complex
Building C1, 5th Floor
Erbil, Iraq
Phone +964 (0) 66 219 3323

Baghdad
Al Mansour, Al Amirat Street
District 601, Street 15, Villa no. 41
Baghdad, Iraq
Phone +964 (0) 770 694 6554

Jordan
Amman
Jabal Amman
190 Zahran Street
P.O. Box 248
Amman, Jordan
Phone +962 (0) 6 550 2200
Fax +962 (0) 6 550 2210

Kuwait
Kuwait City
Dar Al-Awadi Complex
Ahmed Al-Jaber Street, Sharq
P.O. Box 20174
Safat, Kuwait
Phone +965 2240 8844
Fax +965 2240 8855

Lebanon
Beirut
Arabia House
131 Phoenicia Street
Ain Mreisseh
P.O. Box 11-961
Beirut, Lebanon
Phone +961 (0) 1 364 700
Fax +961 (0) 1 369 820

Libya
Tripoli
Tripoli Tower
P.O. Box 93645
Tripoli, Libya
Phone +218 (0) 92 370 1049

Oman
Muscat
Minaret Al Qurum Building, 6th floor
Qurum Area, Muscat
P.O. Box 258
Ruwi, Postal Code 112
Muscat, Oman
Phone +968 (0) 2481 7775
Fax +968 (0) 2481 5581

Palestinian Territories
Ramallah
Al Mashreq Insurance Building
P.O. Box 447
Ramallah, Palestinian Territories
Phone +970 (0) 2 295 4714
Fax +970 (0) 2 298 4703

Qatar
Doha
Al Ahli Bank Building
Sheikh Suhaim Bin Hamad Street
P.O. Box 431
Doha, Qatar
Phone +974 (0) 4434 1112
Fax +974 (0) 4442 2131

Saudi Arabia
Riyadh
Prince Turki Bin Abdullah
Al-Saud Street
Sulaimana Area
P.O. Box 213
Riyadh 11411, Saudi Arabia
Phone +966 (0) 1 282 8400
Fax +966 (0) 1 282 8428

Al Khobar
ABT Building, Al Khobar
P.O. Box 182
Dammam, Saudi Arabia
Phone +966 (0) 13 668 5700
Fax +966 (0) 3 887 3931

Jeddah
The Headquarters Business
Park Tower
40th floor, Corniche Road
P.O. Box 442
Jeddah, Saudi Arabia
Phone +966 (0) 12 578 1000

Sudan
Emaar Square, Building 3, level 6
Downtown Dubai
P.O. Box 4254
Dubai, United Arab Emirates
Phone +971 (0) 4 376 8888
Fax +971 (0) 4 376 8899

United Arab Emirates
Abu Dhabi
Al Sila Tower, 11th floor
Abu Dhabi Global Market Square
P.O. Box 990
Abu Dhabi, United Arab Emirates
Phone +971 (0) 2 408 2424
Fax +971 (0) 2 408 2525

Dubai
Emaar Square, Building 3, level 6
Downtown Dubai
P.O. Box 4254
Dubai, United Arab Emirates
Phone +971 (0) 4 376 8888
Fax +971 (0) 4 376 8899

Fujairah
Al-Fujairah National Insurance Co.
Building, 6th floor
P.O. Box 462
Fujairah, United Arab Emirates
Phone +971 (0) 9 222 2320
Fax +971 (0) 9 222 5202

Ras Al-Khaimah
Julphar Commercial Towers, 19th
floor
P.O. Box 435
Ras Al-Khaimah, United Arab
Emirates
Phone +971 (0) 7 227 8892
Fax +971 (0) 7 227 7465

Sharjah
United Arab Bank Building, 13th
floor
Al Buhairah Corniche
P.O. Box 5470
Sharjah, United Arab Emirates
Phone +971 (0) 6 517 9500
Fax +971 (0) 6 517 9501

Yemen
Sana'a
Sana'a Trade Center
Algeria Street, Sanaa
P.O. Box 15655
Alsafyah, Yemen
Phone +967 (0) 1 448 374
Fax +967 (0) 1 448 378

Quick links

Website
deloitte.com/middleeast

LinkedIn
Deloitte

Facebook
Deloitte

Twitter
@DeloitteME
@DeloitteMEjobs
@DeloitteKSA

Instagram
deloittemiddleeast

WorldClimate

Climate change
is not a choice.
It's billions of them.

Connect at www.deloitte.com/worldclimate



Deloitte.



This publication has been written in general terms and therefore cannot be relied on to cover specific situations; application of the principles set out will depend upon the particular circumstances involved and we recommend that you obtain professional advice before acting or refraining from acting on any of the contents of this publication.

Deloitte & Touche (M.E.) LLP ("DME") is the affiliate for the territories of the Middle East and Cyprus of Deloitte NSE LLP ("NSE"), a UK limited liability partnership and member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL").

Deloitte refers to one or more of DTTL, its global network of member firms, and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms are legally separate and independent entities. DTTL, NSE and DME do not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 300,000 people make an impact that matters at www.deloitte.com.

DME would be pleased to advise readers on how to apply the principles set out in this publication to their specific circumstances. DME accepts no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

DME is a leading professional services firm established in the Middle East region with uninterrupted presence since 1926. DME's presence in the Middle East region is established through its affiliated independent legal entities, which are licensed to operate and to provide services under the applicable laws and regulations of the relevant country. DME's affiliates and related entities cannot oblige each other and/or DME, and when providing services, each affiliate and related entity engages directly and independently with its own clients and shall only be liable for its own acts or omissions and not those of any other affiliate.

DME provides audit and assurance, consulting, financial advisory, risk advisory, and tax services through 27 offices in 15 countries with more than 5,000 partners, directors and staff.