

# € TRAINING

Fintech School



10 - 14 November 2024  
Sharm El-Sheikh (Egypt)  
Sheraton Sharm Hotel,  
Resort,



## Fintech School

REF: T2038 DATE: 10 - 14 November 2024 Venue: Sharm El-Sheikh (Egypt) - Sheraton Sharm Hotel, Resort, Fee: 3520 Euro

### Introduction:

This training program offers comprehensive education and practical skills development in the rapidly evolving field of financial technology. Through expert-led instruction and hands-on learning experiences, participants gain insights into fintech trends, strategies, and innovations shaping the future of finance.

### Program Objectives:

At the end of this course, participants will be able to:

- Navigate the intricate landscape of financial technology with confidence, understanding key concepts, trends, and emerging technologies.
- Apply theoretical knowledge to practical scenarios, leveraging fintech tools and strategies to solve real-world challenges in finance.
- Collaborate effectively within multidisciplinary teams, contributing valuable insights and driving innovation in the fintech ecosystem.

### Targeted Audience:

- Finance professionals with varying levels of experience to Islamic Finance. Entrepreneurs.
- Corporate executives.

### Program Outline:

#### Unit 1:

##### Financial services and digitalization:

- How technical and societal factors of the twenty-first century affect customer expectations defining characteristics of the digital age. include hardware advancements, cloud computing, or 5G.
- How to deal with legacy in workers, customers, processes, and technology.
- How to use partnerships and new technology to compete on equal footing with modern-day rivals.
- Why data juggernauts are attempting to enter the finance sector, what chance they have of succeeding, and how to defend your company.

#### Unit 2:

### How to ride the ntech wave:

- Pertaining to upcoming banking business models.
- Concerning the significance of the banking license and the stability of this entry barrier.
- Pertaining to changing customer attitudes and the needs for financial services.
- Why Asian companies are outperforming their Western counterparts by a wide margin.
- Specifically, the infrastructure, platform, and application are the key participants at each level.
- Using tools like technology watch to determine the best adoption path and timing.

### Unit 3:

#### Blockchain essentials:

- Introduction to cryptocurrency, blockchain, distributed ledger technology DLT, tokenization, and smart contracts.
- A new techno-economic paradigm is emerging, made possible by the widespread and inexpensive "trust" that has emerged as the new essential resource.
- It will affect your company in both direct and indirect ways.
- A step-by-step guide on when a blockchain makes sense for your business and what kind of setup to utilize as a foundation.

### Unit 4:

#### Blockchain for banking and nancial services:

- What major facets of governance are impacted by the blockchain, and what can use cases teach us about them?
- How the blockchain can alter business models in finance and create new revenue streams is one of the blockchain tactics that financial institutions are pursuing.
- What competitors are most likely to undermine banks' pro t pools using blockchain technology, and how can this be stopped?
- What are lawmakers, regulators, and central bankers working on?

### Unit 5:

#### Cybersecurity in the Financial Sector:

- Understanding the evolving landscape of cyber threats in the financial sector, including phishing attacks,

ransomware, and insider threats.

- Implementing robust cybersecurity protocols to protect sensitive customer data and financial assets in an increasingly digitalized environment.
- Exploring the role of artificial intelligence and machine learning in enhancing cybersecurity measures and detecting potential breaches in real-time.
- Collaborating with regulatory bodies and industry peers to establish industry-wide cybersecurity standards and best practices.
- Developing comprehensive incident response plans to mitigate the impact of cyber attacks and ensure business continuity in the face of potential breaches.