Deep Science Publishing
https://doi.org/10.70593/978-93-49910-19-5_11

DeepScience
Open Access Books

Chapter 11: Integrating FinTech innovations, APIs, and open banking frameworks into legacy systems

11.1. Introduction to FinTech Innovations

FinTech encompasses a vast array of technological innovation driving change in the world's financial systems. Innovations are reshaping financial services, including areas like lending, payments, capital markets, insurance, and wealth management. The initial wave of FinTech innovations focused on improving the traditional banking experience by leveraging technology to allow users to handle banking tasks more easily. Startups built products to simplify and facilitate online payments. Similarly, some companies helped drive the adoption of online dining reservations, while others focused on automating expense reporting (Drasch et al., 2018; Gozman et al., 2018; Oliveira et al., 2019).

In recent years, however, FinTech innovations have made more profound modifications to the way financial products are created and offered. Some FinTech companies are replicating investment and transaction banking models – disrupting and decentralizing traditional banks by offering lower-cost products directly to consumers. Others are providing financial services to underbanked populations. At the same time, financial technology has had important effects outside the realm of traditional financial companies. The adoption of social networks has begun to alter the nature of financial products, and advances in analytics and artificial intelligence are pointing the way toward new capabilities for credit scoring, risk management, and automated trading. Additionally, the financial technology ecosystem is rich and varied. Its participants range from established financial companies investing heavily in technology to create optimal products to start-up technology companies aiming to transform particular sectors of

financial services into easily accessible online experiences. Through finance-focused innovations, the entire FinTech ecosystem contributes to an era of historic change in the financial services industry (Zachariadis & Ozcan, 2017; Vives, 2019).

11.1.1. The Evolution and Impact of FinTech Innovations

Rapidly evolving financial technologies, FinTech, are changing how finance services are delivered both by renewing the existing service deliverers and providing alternative services. New services are either innovative versions of existing solutions or entirely new ones and are provided by novel kinds of companies, many of which did not deal with financial services before, and are called disruptors. By using the term disruptors, we are referring not only to fintechs but also to those tech companies offering financial services. Disruptors provide alternative solutions to credit, payments, and investments among others, and their customers benefit from lower fees, greater efficiency, and better user experiences. When compared to traditional financial service providers like banks and fellow disruptors, financial solutions become more attractive to customers and thus gain market share. This shift is referred to as the disintermediation of the financial industry.

Fig 11 . 1 : Mastering Open Banking Integrations

FinTech can be found in several areas. Payments FinTech focus already on developed areas. Other financial solutions are heavily utilized like robo-advisors in investment

management. Platforms around cryptocurrencies are still entering the market. Even traditional back-office processes can be found in new and efficient versions provided by FinTech. The impact of regular FinTech does not stop at disrupting the existing services but extends to new forms of service delivery. For example, InsurTechs provide an entirely new market for comparison websites where customers just need to add some information and receive a list of service levels and prices of various insurers. Similar strategies can be found in wealth management which has made the disintermediation process easier for regular customers.

11.2. Understanding Legacy Systems

Legacy systems play a critical role in the day-to-day business operations and strategic mission of financial institutions. The term "legacy technology" encompasses the IT assets—hardware, software, databases, and interfaces—that have become essential elements in the maintenance of routine bank functions, from payment systems to customer information and record keeping. These vital systems are usually difficult to manage and costly to maintain because the knowledge needed to tweak, support, and govern them is typically scarce. The systems that banks use to provide services to their customers, including more known processes like ATMs and debit cards, are often decades-old proprietary software built and maintained by legacy providers for banks covering essential banking functions, such as core deposits.

The legacy environment also includes banks' clients. Eighty-six percent of bank account holders have been with the same bank for more than five years; one in three has maintained an account with the same institution for 25 or more years. Customers tend to become comfortable with the processes—branches, online banking, and mobile access—that banks establish. These processes are typically highly regimented, tightly regulated, and somewhat inflexible. Changing a bank customer’s payment options or modes can be difficult, particularly if the customer has a credit card or merchant account. Bank legacy systems are not only expensive and inflexible, but they are also critical to bank operations of reaching and servicing customers. As a result, banks tread carefully when evaluating and adopting wholesale changes to their legacy payment systems.

11.2.1. The Significance of Legacy Financial Systems

About three decades ago, it was stated that "But every organization that utilizes large scale computer systems has invested heavily in capital-intensive legacy systems. The reasons that such enterprise-level systems are not abandoned are many. Two commonly cited arguments are that the systems are too complex to understand and that the costs of replacement would outweigh the costs of operation even though the systems might be

technologically outdated." I do believe this is still the case. These systems are crucial for the enterprise critical functions and systems that are in daily use. They are reliable, guarantee operational stability and high security. The loss rate for all enterprise systems in general, and legacy systems in particular, is extremely low. In regard to this extremely low loss rate, the utilization frequency of legacy systems is very high. In the financial sector, these systems are loss rated extremely low. In regard to this extremely low loss rate, the utilization frequency of legacy systems is very high. The monetary loss rate for financial services are not close to other economic areas.

Some banking services are to the extent more than 300 years old. They are essential for financial transactions which are in global use every day, like interbank payments, custodian and clearing services, currency exchanges, stock market exchanges, and mortgage financing. A discrepancy in central finance structures leads to a loss of customers and reinforces the perception that banks are not competent in digitalization and technological developments. This has a contagious domino effect. A feeling of uncertainty and a lack of confidence are created for business services. The failure of a corporate customer can have an impact on the entire banking system, especially when it is about a large company. The main point is that existing customers may resort to other solutions or other banks for their business.

11.3. The Role of APIs in Financial Technology

One of the terms that come up in this book is "API". API stands for Application Programming Interface. In simple terms, an API is a set of protocols and tools for building software applications. It specifies how software components should interact and is used when programming graphical user interface components. More realistically, an API is a code that allows two software programs to communicate with each other. In other words, an API is an intermediary or a messenger that allows two different applications to communicate with each other. It also allows different parts of a system to communicate with one another. APIs can be compared to a restaurant's menu, which lists various dishes that customers can order. The customer does not have to know how to prepare the food; they simply have to choose and order a dish from the menu. The restaurant's kitchen uses the order as an API to prepare the dish.

By the same token, an API allows a particular product or service to communicate with other products and services without the need for a user interface. In fact, the user is barely involved in the background. APIs can be classified into several types: the types of data access methods and other protocols used to transfer data. For example, a data access API can be based either on Remote Procedure Call or Message Oriented Middleware. An API can also be classified into those that are exposed to the customer so that the customer can enhance or leverage those interfaces in their applications and those that are used

internally. Another classification of APIs is based on how they are packaged. Some APIs come as part of the product while others are external to it.

APIs are the lifelines for modern businesses. They help link diverse technologies and functions to deliver a seamless user experience. Companies take advantage of APIs to capitalize on the digital economy. With APIs, banks expand their business models and revenue sources by allowing third-party developers to create innovative apps and services that leverage their data and services. Benefits of API Integration include: Business Growth: It creates numerous opportunities for business partnerships and expansions. Cost Savings: It minimizes the cost of new application development. Improved Efficiency: It makes use of the preferred tools and technologies over the existing applications. Improved Security: It provides an added layer of security for enterprise systems over the APIs deployed. Improved User Experience: The target users can use innovative and useful solutions.

Innovation: Organizations can create innovative offerings through the parameters or replication of others' innovative solutions. Product Differentiation: Companies can integrate enhanced, specific services that meet user needs. Improved or New Customer Relationships: APIs provide a new channel or route for reaching customers.

11.3.1. API Definition and Types

The Internet has been built on top of Application Programming Interfaces (APIs), the data inference points that are available over the Internet that connect systems together and provide services. Clouds, social media platforms, and other services depend on APIs to allow consumers to connect to their services. For financial services, APIs are a way to connect to other systems that offer services such as deposit, trading, market quotes, payments, and others. In addition, APIs allow connect services to other systems such as accounting, enterprise systems, fraud detection, and compliance. APIs extend a financial institution’s services to third-party developers. This allows for more product offerings than the financial institution has resources to develop. Furthermore, new systems can be built quickly using templates.

An API is a business function that someone else has exposed in a standard way to outside developers. Examples of APIs include various social media APIs, e-commerce APIs, and any of the cloud APIs. These APIs expose services like functionality for connecting to the network sharing functions, data retrieval or data storage, or storage, computation, database, or networking services. APIs can provide access to different platforms, processes, or products. Examples include account verification, deposit access, transaction processing, payments, document capture, compliance processes, document pagination, compliance, and fraud detection. In addition, APIs can extend every aspect

of the customer and vendor network. An API can serve customers at any stage of the customer lifecycle and support and extend any service that a vendor provides.

11.3.2. Benefits of API Integration

Today's financial institutions are increasingly turning to financial technology companies to modernize their products, services, and distribution platforms. However, the legacy systems that make up their back office environments can delay efforts to modernize and slow sales from new distribution channels. Enter Application Programming Interfaces, which let institutions integrate and extend the capabilities of their existing systems on an incremental basis, while improving speed and agility. As a result, marketers can more rapidly respond to changing consumer demands with innovative products, services, and features.

The benefits of developing open, connected ecosystems using API-enabled integration strategies are numerous. For financial institutions, the most immediate is cost reduction. APIs can simplify the process for building and integrating new products and services. A bank or credit union can use APIs to connect to third-party services as a way to offer innovative features like budgeting or identity monitoring. It's a way to enhance—and not necessarily replace—current offerings.

Speed is another major benefit of API integration. APIs can drastically reduce deployment times for new services, as workflows can be created using pre-existing services from third parties. Products can be brought to market more quickly and resources can be allocated more efficiently. With APIs and microservices, financial institutions can work on specific pieces of functionality in parallel, speeding up the development workflow and reducing time to market. This is particularly beneficial in the fast-paced space, where marketers can't afford to wait months or years for new releases to reach customers.

Finally, an API strategy also can improve the quality of new products and services. APIs can eliminate many of the manual processes that cause errors to occur. Since APIs and microservices are utilized across projects, the services can be thoroughly tested for quality issues before release. By using APIs developed by other companies, the manufacturer can also take advantage of a unique capability. Most companies will seek out third-party manufacturers that are experts in specific areas when looking to develop core competencies, and APIs enable companies to connect with those experts.

11.4. Open Banking Frameworks

This chapter provides a concise overview of the Open Banking domain. At first, it presents a definition of Open Banking, followed by its regulatory landscape and finally, it concludes with a description of the main participants in Open Banking, the platform ecosystem. Before describing the chapters, however, and to facilitate a quicker overview of key concepts, we will present Open Banking architecture and use cases.

Open Banking allows third parties to build new financial products and services with the customer's consent, through the secure sharing of customer information via merchant and third-party developer-friendly Application Programming Interfaces. Open Banking architecture is based on third-party developers building financial solutions including software as a service solutions for customers, with Bank ecosystem partners providing customers with data, transaction, and other information security and reliability. These Bank security and reliability services include Customer Personally Identifiable Information, Account Sharing and Data Privacy, Transactional and Service Data Protection, Dispute Resolution and Transaction Safety, and Insight Providers.

11.4.1. Overview of Open Banking

Open banking is the practice of allowing access to consumer banking, transactions, and other financial data from banks and nonbank financial institutions through the use of application programming interfaces. In open banking, consumers are empowered to allow third party developer applications and services to access their financial information. For instance, first party apps can inform users about their spending habits, remind them about pending bill pay and reloadable debit card transactions, or help them pay down debt by automatically transferring money to savings accounts. In this domain, third party developers can help banks gain market share by creating better financial tools, or speed up the creation of consumer-facing apps. In some sense, open banking is a natural evolution of electronic banking and mobile banking. These two products relied heavily on electronic systems that managed internal transactions. In contrast, open banking expands this access to include third parties including fintechs that use consumer consent to develop applications that interact with a bank's existing information technology. Through the use of APIs, bank data is securely shared with third party applications that consumers choose to use. Modern-day consumers expect real-time banking access and responsiveness. Banks can engage consumers and enhance their spatial experience through the creation of applications accessible through open APIs.

11.4.2. Regulatory Landscape

The regulatory landscape for open banking initiatives is still evolving. Although many jurisdictions had enacted privacy laws long ago, compliance with data protection regulations was, until very recently, a fairly low bar. Data subjects had limited rights, and regulatory enforcement waned with the exceptions of high-profile predatory privacy practice cases. A major shift began in 2018 with the introduction of new regulations that mandated that banks only provide customer bank data to registered third-party providers at a customer's request. Elements of these initiatives are emulated in many other countries around the world. The bottom line is that financial institutions, third-party providers, and consumers (whose records may be shared under open banking) must all comply with strict regulations that stiffen penalties for privacy violations.

Some enforcement will be state-federal coordination with states adopting their own open banking initiatives; other enforcements may follow existing lines of authority created by preemptive federal statutes. Some states may go even further, by introducing laws and regulations that require stricter security and privacy measures than the existing federal laws. For instance, certain state laws serve as a wake-up call for companies doing business with residents that have weak privacy practices, pointing to the consequences for businesses that avoid compliance for privacy violations.

On the industry side, relevant standards organizations have taken the lead in establishing the necessary requirements for third-party apps. Published frameworks provide developers of financial services applications with guidance. The objective of these documents is to encourage consistent, industry-wide best practices for secure development.

11.4.3. Key Players in Open Banking

Open Banking is an initiative that provides certain third-party financial service companies with direct access to consumer bank accounts via the open application programming interfaces of banks. Banks and the Open Banking Implementation Entity are the key players in Open Banking. FinTech companies aggregating and analyzing data are also recognized as important stakeholders in the Open Banking ecosystem. A complex set of exchanges will exist between banks, third parties, and customers. Banks will be likely to charge third parties account fees to access banking data and consumer transactions. The Open API model will enable the bank's customer to direct how and with whom their financial data is shared. Specifically, the customer will give consent to the bank for a FinTech firm to connect to the Open API to develop new payment and data aggregation services. In return, the FinTech firm will either charge the customer for the service or gain revenue from a deal with the bank. Rewarding FinTech for creating

services that enhance customer experience should promote competition in the industry, which will be good for consumers.

Fig 11 . 2 : Players in Open Banking

Key Issues. The ongoing concern in the financial services sector is the need for protection and maintenance of consumer privacy and the security of sensitive account data. Consumers must also have opted in to allow their data to be shared between the banks and third-party FinTech companies before data sharing can occur. Also unresolved are who gets and keeps the customer relationship—the bank or the third party. When customer data is used by FinTech to offer a better product to a prospective banking consumer with the price of the product discounted to win the customer's business, both are providing a service to the consumer. However, the traditional bank may not see it that way if it loses that customer.

11.5. Challenges in Integrating New Technologies

There are several challenges related to the manner in which new technologies are integrated into banks' business processes and IT ecosystems. Financial services institutions may be pressured to adopt the latest technology or innovative partnerships to remain competitive. Regulators often step in to define technology rails to promote resilience, reduce risk, or facilitate security. In addition to these demands, there are several challenges specific to banks. Legacy systems, built over decades, make it incredibly difficult for banks to innovate quickly. Long product planning cycles mean

that integrating a new technology, even if it lives on a separate server, takes an exhaustingly long time and can easily break a significant bank product that is part of the daily lives of millions of users. As a result, banks often struggle with being perceived as unresponsive to competitor innovations, angry at customers who expect cool new experiences. In some cases, banks may hold back providers by refusing to publish APIs in a timely manner or without adequate documentation or support. The volume of customer calls that may follow, the day after a third-party company launches a new credit card or credit score optimizer based on bank data, has driven banks to be more responsive. However, a business model that encourages these startups to monetize their initial technological innovation – while offering little in terms of operations or customer service – also subjects banks to the risk of the venerable Innovator's Dilemma. The wave of regulatory involvement in the United States – from pseudo-open banking requirements to data funding rules to ongoing security and data use audits mandated by state legislatures – also creates a further challenge. From the perspective of the average progressive member of a bank's compliance team, the banks could commit resources to either innovation or audits, but not both. With novel technologies making auditors' jobs a lot harder, compliance teams often call for further study under the guidance of vendors specializing in risk to evaluate third-party compliance, artificial intelligence technology for lender decisions, and anti-competitive bias or discrimination.

11.5.1. Technical Barriers

There are many technical considerations when connecting FinTech innovations to legacy systems. These issues generally split into two main areas. The first area includes the existing ecosystem used by the institution and the volume of changes that need to be made in the legacy systems for integration. The second area contains middleware technologies that allow for additional simplifications and facilitate the connection of the disparate components.

Large institutions have multiple legacy systems and databases. They have integrated their operations with internal and external institutions' applications, making substantial changes to any of the systems difficult. To be able to support integration with FinTech corporations and ensure the required functionality, security, and reliability, large and medium-sized institutions need to modify the existing legacy system. Such changes can include implementing API services; modifying direct database connections and exported services; extracting, transforming, and loading the data into other formats; and updating the security features to enable access control and monitoring.

To support the changing ecosystem and to facilitate integration with FinTechs, institutions have created middleware technologies. Middleware technologies can be divided into three main categories. The first category groups API management tools that

provide developers with documented, usable API services. These tools typically support usage tracking and monitoring. The second category of middleware technologies supports the seamless routing of standardized data components between disparate legacy systems and databases. These types of tools simplify and streamline the establishment of the connection of disparate components, enabling speedier integrations. These tools often enable rapid prototype testing and iterative development over time.

These two middleware technologies can solve the majority of technical issues with standardized FinTech service delivery and integration. However, several other issues still need to be addressed. These issues include a wide variety of internal enterprise-formatted data and multiple disparate legacy components, many of which may not use standard protocols or data formats, limiting the usage of off-the-shelf or hosted API management and routing systems.

11.5.2. Cultural Resistance

Any integration of innovative systems into an existing digital ecosystem is a catalyst for social and organizational change. The integration of FinTech, existing banking models, as well as the creation of new business processes represent transformations of traditional productivity methods, which can affect various stakeholders, from employees to external contractors. Internal employees are often the greatest resistance to implementing these types of technological projects. This is because any new technological framework has a disruptive effect, often changing the jobs of the internal technical divisions in charge of these existing services. The objection of these services can range from organizational difficulties in adapting to the new model to technical doubts specific to the service that are often not justified.

In addition to internal resistance, the relationship with external subcontractors that support central banking services can also be a weak link in the chain. A slow adaptation of the external service provider model, which usually has rigid operational and business constraints, can represent a blockage of a new technological system, making it infeasible and difficult to implement. It is essential to define together with external partners the multichannel integration model; too many limitations or a distrust of technological innovation proposed by the main bank can completely derail the project. Finally, customers represent the last link in the chain of integrating new Fintech technologies with existing banking models. Although current technological advancements allow for rapid, at times adaptation to system changes, it is important that customers quickly acquire new operating methods, accustomed as they are to the previous systems.

11.5.3. Compliance Issues

The financial services sector is one of the most strictly regulated environments in commerce. New entrants into this space are necessarily subjected to an equally strict set of regulations as their more traditional competitors. These regulations cover all aspects of the financial service value chain and partner on which FinTech companies often depend on outsourcing segments, as well as being subject. Even where specific compliance issues may not directly arise between the FinTech startup and the local regulators, transaction service providers may be impacted; thus creating a domino effect where all involved will struggle to integrate the desired technology.

The second key issue often is that regulations may differ in substance from country to country. This raises issues for banks with cross-border operations, as the reach of the regulations may not stop at local borders. Thus, banks must create and maintain systems and controls that can sometimes operate in parallel across multiple jurisdictions but may not be able to effectively migrate or at least simplify operating protocols as technology changes. For instance, burdensome reporting requirements at a sub billion levels for incorporated companies, while regulations do not only revolve around strict knowledge customer and antimoney laundering but also generate many additional risk related to and more recent requirements.

11.6. Strategies for Successful Integration

Integrating FinTech innovations into legacy systems presents specific challenges that touch on issues such as service disruptions and data inconsistencies. This means that the approach must be cautious and well adapted — that is to say, a phased upgrading with a clear roadmap is crucial for a successful legacy operational overhaul. Here, we outline some basic steps for a successful integration.

Before beginning the integration or upgrading process of a legacy information system, it is crucial to perform inventory work in order to assess the functionality of the current system in order to identify the technical and operational requirements that must be fulfilled. This activity takes place in collaboration with business specialists who are the system's key users. This allows you to avoid surprises once the integration is completed and to ensure that the new system meets both technical and operational requirements. After assessing current systems, it is possible to start the preparation of a consolidation strategy. The latter has to take into consideration the regulatory requirements that the financial institution has to be compliant with during the whole integration process, the functional and technical requirements of the legacy systems, their architectural and data dependencies, the difficulties around data transfer, and the willingness from business Centers of Expertise to adapt to new services. There are several approaches to a legacy

architecture overhaul, such as one-by-one service updating, data and connectivity scraping, or wholesale ripping and replacing. Each has its pros and cons and must be discussed with the business Centers of Expertise.

Once the migration strategy has been defined, it is advisable to implement a sandbox on which business users will run some tests on the new system. In this validation phase, business Centers of Expertise will try out the new system and validate that it gives equivalent results to the previous one before it is put into production. After these validation tests have been completed and once the two systems are operational at the same time, actual migration tests will be conducted and monitored together with the relevant teams.

11.6.1. Assessment of Current Systems

Assessing legacy applications and foundational systems is the first step in the integration process. Your assessment should map the layout of existing systems, looking for strengths, weaknesses, bottlenecks, and redundancy. Assess your existing tools, capabilities, and workflows as well. Your entire technology stack, including hardware, software, customer base, and third-party vendors will need examination. You'll need to plan an in-depth assessment because it will help you decide what needs upgrading, what systems can no longer serve your organization and your clients, and what systems can remain while integration readiness occurs. Systems that are more flexible will be easier to upgrade or even possibly swap out. Systems that are rigid may need to be replaced or heavily redesigned to allow for the integration of financial technology innovations.

Data is the most critical component in this assessment. The quality, consistency, and timeliness of data will determine what moves forward into the new system, stay in legacy, or be turned into a new data focus entirely. Integrators should develop and document, using flowcharts and diagrams, existing business processes that are dependent on data flows and database services. You also need to find out where the most changes are anticipated from and investigate those data processes more closely. You'll also want to retain access to your old data so that it will be available for historical reporting and business decisions post-migration, but not affect real-time operations. This historical need gives path to many traditional data warehouse capabilities, either in cloud options or through the utilization of sticks and storage arrays. In addition, when integrating with modern approaches such as open applications and APIs, integrate only the specific capabilities that take advantage of data access and manipulation that these methods present.

11.6.2. Developing a Migration Plan

Having completed the assessment of current systems, and having the knowledge of available options and requirements at its disposal, the organization is ready to develop a migration plan. The migration plan should consider each of the organization's legacy systems, minimize impacts on business continuity, and come to grips with how to deal with the organization's ongoing efforts to keep adding value to the legacy systems. At this stage, there are more questions than answers. How long will it take? Which systems get decommissioned first, and how will the connections between systems be managed? What legacy system skill sets will future staff need, and how will that work with current staff skills be managed?

Determining which system gets decommissioned first may involve considerations of business value. First, because the answer may not be obvious, it would be helpful to develop a framework for answering the questions. A simple framework involves answering the following questions for each legacy system. Is the existing system meeting current business requirements? Does the system meet the "need?" Is the current state of the system able to continue delivering needed business functionality? How well is the system performing? Are the system's response time, reliability, and throughput meeting business needs? Does the system have critical, exploitable, or unexploitable vulnerabilities? Are the cost and skillset considerations for keeping the system running acceptable, in terms of effort or cost of workarounds for pain points, such as manual spreadsheets? What is the cost of decommissioning? If the cost of migrating to one of the alternatives is small compared to the decommissioning cost, then there may be a compelling case for just getting through with it.

11.6.3. Testing and Validation

A successful integration of technologies introduces different vendors, products, and layers of technology into a single, cohesive platform. Because FinTech APIs have multiple components with complicated dependencies for key functionality, and performance, load, security, and failover values differ across sub-components, organizations must test each layer thoroughly in best-case and worst-case scenarios, and hope that once deployed in production, the layers will work as expected in special use cases, such as during a market panic or holiday rush, and when exposed to malcontents. Fortunately, testing across layers has its own ways of preventing problems. Testing tools have matured such that they can easily simulate load balancing and failover. Vendor systems have documenting tests that measure input and output timing and performance. Regulatory compliance and security rehearsals, whether done in mock crisis mode with loud alarms or routinely at odd hours, are often independent of the more mundane use case focus of functional testing. Vendors likely have established security protocols. In

addition, FinTech vendors have worked with regulatory authorities to promote better models for best security testing. Recommendations include publishing tools that conduct synthetic transactions — either tests using a robotics scripting technique to create a user transaction — or synthetic reports on input and output timing. APIs often provide sample data for such transactions as well as recommend timing. Reports show statistics such as completion timing for single transactions, per sample data item, aggregated for multiple transactions, and maximum and minimum timing, as well as error rates for all items. APIs have multiple components with complicated dependencies for key functionality, and performance, load, security, and failover values differ across sub-components, organizations must test each layer thoroughly in best-case and worst-case scenarios, and hope that once deployed in production, the layers work as expected in special use cases, such as during a market panic or a holiday rush, and when exposed to malcontents.

11.7. Conclusion

Final Thoughts and Future Directions in FinTech Integration

The constant demand of consumers for new functionalities and experiences, along with the constant introduction and improvement of FinTech-driven capabilities is creating new expectations from banks, insurance and pension service providers, that need to deliver more than regulatory compliance, to guarantee consumer trust and engagement. The introduction of Open Banking frameworks is the privileged vector for established financial institutions, to revitalize their value proposition, while sustainably monetizing third-party innovations delivered via their APIs. However, in order for banks to be able to provide their APIs as the user journey becomes demanding, enabling personalized experiences across multiple touchpoints and involving complex event chaining and algorithm-driven decision algorithms, banks need to be able to deliver a more extensive set of banking transaction-related services on-demand at the user front-end, and in a simpler, more efficient and faster way at the back-end layers.

Legacy systems (not only technology, also in the way they are organized, the way they operate) are naturally well adapted to the traditional business model that they have served banks with, for a long period of time. They are, however, blind to the enormous evolution of regulatory compliance, from simple money laundering checks to the involved privacy-related and know-your-customer regulatory checks of current Instant Payment services. They are also blind to the fact that, in a near future, these operationally intense and costly functions will need to be performed in real-time, keeping the transaction risk related to them at an acceptable level, and leaving a small risk of error for banks to deal with, if they want to monetize this avenue as their sole, or main, source of differentiation. In a revolutionized future of retail banking, banks will need to deliver APIs that provide

consumer services at a dependable level of reliability, in real-time and continuously open for business.

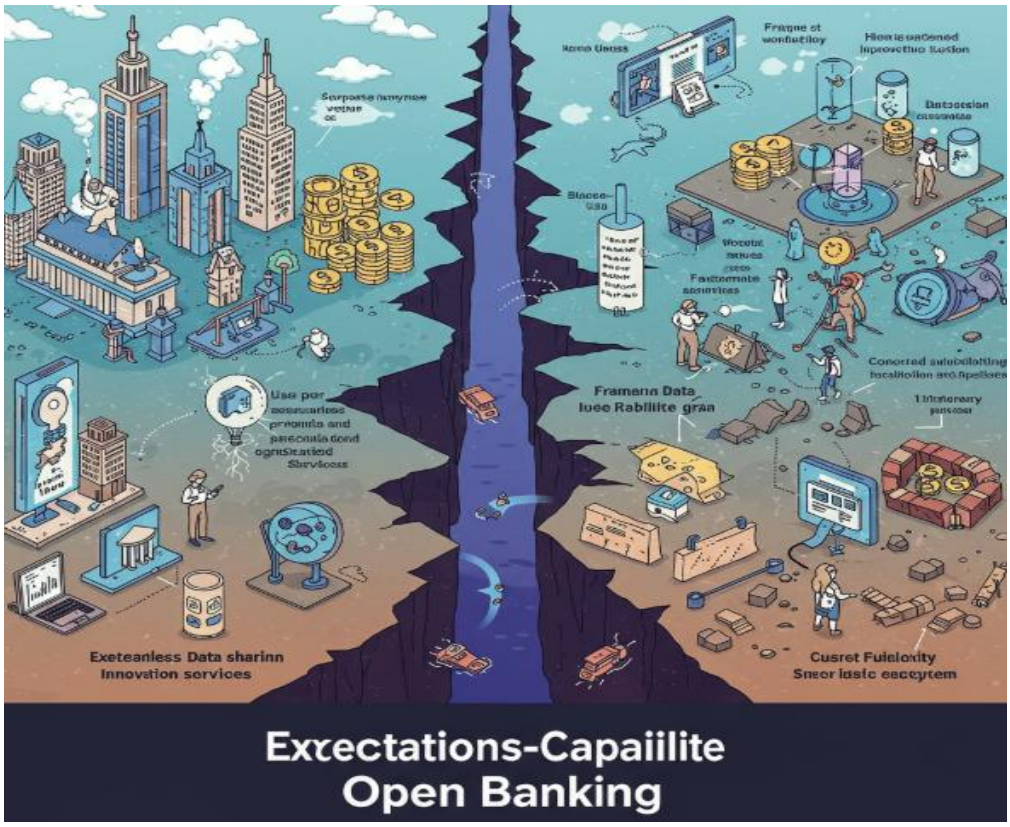

Fig 11 . 3 : The Expectations-Capability Gap in Open Banking

11.7.1. Final Thoughts and Future Directions in FinTech Integration

FinTech innovations, in particular the innovative campers, the deployers are laying a progressive transformation of the financial system by provisioning best of breed functionality to enable financial services anywhere in the global economy and unlocking economic value domestically or internationally. While the phased enrichment of core banking functions via connectors using data exchange is a significant step towards providing and delivering advanced use case implementations, it is not fast enough to meet investor's expectations for quick wins. Hence investor strategies for value realization ranging from bootstrapping to cash cows leveraging legacy systems; to custom-built and sustainable models based on green-field architectures are risked based on the uncertainty of timing and outcomes.

In addition, the ever-shifting scale of risk associated with legacy system utilization and legacy models create further obfuscation for investors, operators, and implementers associated with redirected focus within the external business environment. Regulatory perspective and enforcement mechanisms are effective in protecting against extreme rogue behavior within an external environment. However, the system-based logic for incentivizing, regulating, and orchestrating significant parts of the external environment is on the verge of considerable change due to progressive technological evolution. Hence the question remains - how can an external digital ecosystem intersect with the internal eco-cell, core function, and user experience internally within an organization. FinTech integration appears to be the next stage of commercial and spreading adoption of democratised financial services to realize deliberate financial goals.

References

Gozman, D., Hedman, J., & Olsen, K. S. (2018). Open Banking: Emergent Roles, Risks & Opportunities. Journal of Information Technology, 33(2), 104–117. https://doi.org/10.1057/s41265-018-0054-0

Drasch, B. J., Schweizer, A., & Urbach, N. (2018). Integrating Legacy Systems into a Digital World—A Business Model Perspective on API Management. Journal of Business Economics, 88(3), 337–375. https://doi.org/10.1007/s11573-017-0865-3

Vives, X. (2019). Digital Disruption in Banking. Annual Review of Financial Economics, 11, 243–272. https://doi.org/10.1146/annurev-financial-100719-120854

Zachariadis, M., & Ozcan, P. (2017). The API Economy and Digital Transformation in Financial Services: The Case of Open Banking. SWIFT Institute Working Paper No. 2016-001. https://doi.org/10.2139/ssrn.2975199

Oliveira, T., Thomas, M., Baptista, G., & Campos, F. (2019). Mobile Payment: Understanding the Determinants of Customer Adoption and Intention to Recommend the Technology. Computers in Human Behavior, 61, 404–414. https://doi.org/10.1016/j.chb.2016.03.030