Investment banking:
New paradigms and new forms of technology

Laurent-Olivier Valigny,
HSBC Group

[special issue of *Réalités Industrielles*, February 2019]

Abstract:
The Nora-Minc report on the computerization of French society — now more than forty years old — prophetically compared banks to "tomorrow's iron and steel industry" as it discussed a saturated market, production overruns, insufficient equity, production costs and disruption due to telematics and computers. The current digital revolution has overtaken investment banking — a strange echo of the diagnosis made so long ago despite the fundamentally different contexts. Investment banking has undergone three shocks during the past decade. It had to cope with the 2007-2008 meltdown. The response to this first catastrophe was a massive regulatory shock; and now, investment banks are, after ordinary banks, facing the digital transition. Stemming from several technological innovations (or even revolutions), this transition is a potential source of growth and increasing productivity; but it inevitably entails a cultural change and the adaptation of organizations — processes to be controlled.

The 2008 meltdown: The explosion of data and need for stronger oversight

The brunt of the 2008 financial crisis is worth mentioning from the outset. The meltdown did not lack precedents (1987, the Russian crisis in 1998, etc.), but was unique given the structural changes that, related to it, signaled a paradigm shift: exceptional market volatility, exacerbated price trends, the upsurge of factors related to previously unknown risks, the breakup and dislocation of categories of assets (The very concept of a rate curve came under criticism), loss of confidence in currencies, the dissociation of sources of funding, the differentiation of liquidity costs, and higher risk premiums.[1] In this context marked by uncertainty and increasing computational complexity, the monitoring and steering of activities in financial markets entailed drastic reinforcing the capacities for processing and analyzing data (the frequency of calculations, the granularity and scope of data, and the return of intelligent information).

The meltdown also brought to light fraudulent practices (the manipulation of benchmarks, such as the Libor, or the fixing of exchange rates) and deviant behaviors (rogue trading), all of which made a surveillance of transactions more necessary.

[1] This article has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references.

Regulations about client information and reporting requirements

Given the scale and consequences of this crisis, one response by regulators was to significantly reinforce requirements with regard to standardization, accountability, oversight and reporting. Several regulations were thus adopted.

The Basel Committee on Banking Supervision released a set of "*Principles for effective risk data aggregation and risk reporting*" (BCBS 239). Enforced since 2016 on systemically important financial institutions, this standard stipulates fourteen principles that apply to: governance (data architecture and information technology infrastructure), the aggregation of data (accuracy, integrity, completeness, timeliness, adaptability), risk reporting (accuracy, comprehensiveness, clarity, usefulness, frequency, distribution) and supervisory review (remedial actions, cooperation, implementation).

To promote accountability and competition, the second EU directive on the market in financial instruments (MIFID 2) has decentralized and "fragmented" order books and trading venues by multiplying the methods for executing transactions, whether on financial settlements markets, through multilateral trading systems or by "internalization" (when an intermediary fills its clients' orders from its own inventory or against orders from other clients). In parallel, stronger requirements about information and price transparency in customers are intended to provide and prove that transactions have been executed as best possible. Banks have to collect and transmit information from the relevant markets and explain the methods used to set the fees for the transactions they execute.

These requirements for transparency are based on a codification of the parties and financial instruments involved in a transaction. The purpose of introducing procedures for assigning a legal entity identifier (LEI) to parties in the financial markets is to improve the management and control of the risks to counterparties. This practice was motivated, to a degree, by the difficulty of identifying the exposed legal entities during Lehman Brothers' bankruptcy proceedings. The Dodd-Frank Act passed in the United States requires a unique transaction identifier (UTI) or a unique swap identifier (USI). Likewise in Europe, the European Market Infrastructure Regulation (EMIR) requires a unique identifier for the centralized reporting of uncleared transactions — a requirement that completes the obligations related to the reconciliation of financial statements among counterparties.
These stiffer requirements for compliance focus on identifying the counterparties and updating information about them. The fight against money-laundering or tax evasion, for example, necessitates thorough knowledge of these phenomena and a detailed verification of clients. This information has to be centralized even though it is hard to imagine actually doing this because so many channels of information exist, even within a single bank. For this reason, decompartmentalizing and sharing information is of overriding importance.

Finally, systematically conducting stress tests, which simulate the impact of shocks (macroeconomic or financial, regional, sectoral or global) on items (results, equity, profitability, liquidity) in financial statements provides management and regulators with an across-the-board view of investment bank activities and their risks.

Overall, the collection of information on a large scale, the referencing and storing of data, the systematic exchange of information, the production of reports of an ever finer granularity represent, in terms of the architecture for information systems, strategic and industrial issues.

Changes in technology

The exponential growth in the demand for information is taking place at a time when the offers from technology for satisfying it are also multiplying. The result is a massive, unprecedented increase in the capacity for processing data, both in *1)* in the volume of data available for manipulation and storage and *2)* in the diversity of the available formats (structured data about, for example, transactions or price trends duly recorded in databases, or less standardized data, such as contracts, conversations, electronic messages, satellite images, news bulletins from Reuters, or posts on forums, the social media or other Internet sites).

In this context, cloud computing taps the computational power and storage capacities of remote computer servers via a network, usually the Internet. This remote sharing of processes and of processing facilities results in gains of efficiency.

Blockchains are another, still partially experimental, innovation based on cryptographic computing technology. Though not requiring an authority who centralizes control, a blockchain cannot be falsified. It can be used to safely make and transmit sequential records of the actions of the many parties who share access to the chain. Several uses have been imagined, for internal processes (*e.g.*, accounting books or enhanced due diligence) and for external transfers of information (*e.g.*, international commerce, the trade in raw materials). Promising prospects are arising too in the activities of settlement, delivery, clearing and deposits.

Finally, and mainly, we are witnessing a development of cognitive functions based on the latest techniques of data analytics for visualization, filters, smoothing functions, stratification (data mining), behavioral analytics, predictions, the detection of trends or anomalies, profiling, scoring, ranking…. This allows for an optimization of communications with clients, “smart” marketing, an “enhanced” management and the automation of controls. These techniques use self-learning algorithms (*e.g.*, machine learning) without having to first make a simulation or build a model.

The many fields of use

In practice, automation, even robotization, involves the electronic recording and passing of orders, the matching by algorithms of orders to sell and to buy, the execution, confirmation, settlement, delivery and collateralization of over-the-counter transactions. The most noticeable advances can be seen on standard, organized markets (currencies, cash payments for securities, government bonds).

In parallel, clients’ objectives in terms of investments, coverage, management and funding, as well as the restrictions they impose and changes in their behavior (the history of their stated interests, of the orders filled at their request, and too of the bids they made but that were lost to the competition) can now be recorded electronically, consulted on demand, referenced, crossed and analyzed. The upsurge in smart marketing completes the automation of knowledge about clients, which the processing of electronic financial documents and, in general, the dematerialization of relations between banks and their clients have made possible.

Ultimately, online transactions have been made easier; the identification of prospects has been optimized; and the production of reports has been automated. Thanks to the sharing of libraries of financial calculations, of computational environments and of clients' data, businesses have better connections with each other, and this is conducive to cross-selling. In this respect, digital technology offers an environment propitious to business growth, which is now more client- than product-oriented.

A completely different question — the prevention and detection of attempts to commit fraudulent activities, whether internal or external — brings to mind the techniques for processing weak signals: trend analyses, detection of behavioral biases or abnormal patterns in the execution and/or recording of transactions, the identification of suspicious transactions, automatic warnings…. These activities rely on stronger electronic surveillance.

New forms of technology, new players

For investment banking, this electronic environment is not just an opportunity but also an ardent obligation because the competition — existing and new (FinTechs) — has adopted it. As Lloyd Blankfein, CEO of Goldman Sachs, declared: "*We are a technology firm. We are a platform.*"

Whereas universal investment banking historically drew up multimarket strategies for integration and synergy, FinTechs have adopted niche strategies for rolling out advanced forms of technology in highly targeted market segments, such as the platforms for filling orders or managing collateral, where the speed of execution, postmarket automation, an optimized customer-vendor interface, and low production costs yield competitive advantages.

Competitors, indeed, but also partners: investment banks are becoming users of what FinTechs have to offer. They are setting up joint ventures and business incubators, and are raising funds for these startups or organizing direct investments.

Major organizational and human consequences

First of all, the permeability of information now means that production jobs are no longer to be seen as routine processes performed vertically in bunkers, but instead as flows of shareable, adaptative, multiform information streaming through an open ecosystem where communication protocols are essential. In the mean time, telework and the relocation or externalization of activities (research, middle office) have become a necessity.

Secondly, the management (identifying, referencing, diffusing) of "information deposits" in investment banking turns out to be a highly strategic activity. Information is literally a raw material for a bank's operations (making decisions, steering projects, managing communications). For this reason, the quite recent position of chief data (or chief digital) officer signals the coming of the electronic age in investment banking.

Human resources are also changing. New job profiles are demanded (in some cases, data scientists instead of pure financiers) that are more collaborative than hierarchical. Information from the job market is also more transparent and available in nearly real time. Social networks like LinkedIn identify potential recruits and target job offers to potential candidates. While making the labor market more fluid, the more frequent recourse to such services might also stimulate occupational

mobility among bank employees and lead to unstable careers. Finally, recruiters are now competing: investment banks, on the one side, and FinTechs or, more broadly Google, Amazon, Facebook and Apple, on the other.

Issues arise in relation to acculturation. How to make employees aware of digitization and train them in digital technology? How to accompany them as they update their technical skills and work methods?

The risks of the digital transformation

This irreversible transformation is not at all free of risks. There are:

- STRATEGIC RISKS. The incompressible rate of failure that will result from the proliferation of initiatives and projects (sometimes experimental) within establishments must be recognized and managed.

- COUNTERPARTY AND INVESTMENT RISKS. Some single-project operators will, for sure, vanish from the market. In this respect, the current enthusiasm for the digital credo reminds us of the Internet bubble at the turn of the century. Appropriate due diligence is a prerequisite for forming partnerships with FinTechs and investing in them.

- TECHNOLOGICAL RISKS. Though promising, smart (self-learning) algorithms carry risks inherent in their design and application. For example, some trading programs have been accused of setting off or accelerating sudden movements in the financial markets (flash crashes on currency or bond markets). This calls for a form of governance robust in terms of traceability and audibility.

- OPERATIONAL RISKS. Nor should we omit the risks of fraud and cybercriminality that have arisen out of the increasing circulation of data. In addition, the use of obsolete applications raises the risk of data breaches or thefts, whence the need for substantial investments to protect or update information systems.

Change in continuity or a historical shift?

Investment banking has a history of changes. We might mention the globalization of finance or the growing sophistication of financial products. However the digital transformation it is now undergoing is a major process, an accelerator inevitably laden with a creative destruction of value and with numerous, sometimes exploratory, possibilities… but a process that should be appropriated and mastered.

Sources

CITI GPS (2018) *The bank of the future: The ABCs of digital disruption in finance*, 124p., available via https://www.citibank.com/commercialbank/insights/assets/docs/2018/The-Bank-of-the-Future/122/.

EYG LIMITED (2015) "Transforming investment banks", 36p., available via http://www.ey.com/Publication/vwLUAssets/ey-transforming-investment-banks/$File/ey-transforming-investment-banks.pdf.

ACCENTURE CONSULTING (2018) "Capital markets technology 2022: Five technology design principles for digital capital markets" available via https://www.accenture.com/t20180124T060525Z__w__/us-en/_acnmedia/PDF-69/Accenture-Capital-Markets-Technology-2022.pdf.

AFME (2018) "Technology and innovation in Europe's capital markets: Current trends in technology and innovation and their impact on the 'investment banks of the future'", 36p., available via https://www.fintech2019.eu/wp-content/uploads/2019/02/afme-pwc-tech-and-innovation-in-europes-capital-markets.pdf.