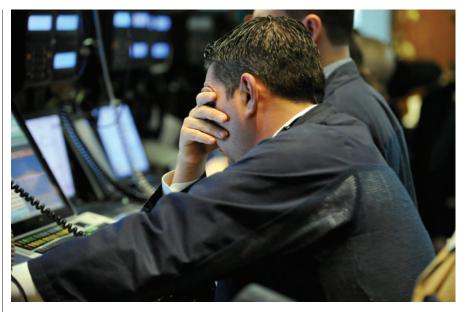# V viewpoints

Roman Beck

Viewpoint
Can IT Lean Against the Wind?

Lessons from the global financial crisis.

THE SEPTEMBER 2009 *Communications* Editor's Letter "The Financial Meltdown and Computing" by Moshe Vardi suggested a link between the financial crisis of 2008 and computing. He is correct to suggest this connection. Information technology (IT) has enabled ever-increased speed and global reach for financial products. Financial institutions in the U.S. and elsewhere have created and deployed complex, structured financial instruments. At the peak of the bull market, the seemingly endless promise of fancy financial products drove the markets to new heights. What went wrong, and what role did IT play? This column cannot provide all the answers, but it offers some recent history and a lesson worth remembering.

The Role of IT in Financial Markets

Before the financial meltdown of late 2008 two important events provided a glimpse into the role of IT in the financial markets. The first was the September 11, 2001 terrorist attack on the World Trade Center. The attack destroyed a prominent symbol of Wall Street. It also destabilized the financial clearing and settlement systems of major banks located nearby. Foreign exchange settlements in U.S. currency collapsed, which could have created a global financial calamity. However, in part because of remedies applied during the Y2K crisis, emergency back-up systems in the IT infrastructure prevented the worst. Within three hours, disas-

ter recovery systems located abroad took over from New York to handle all U.S. currency transactions, and clearing and settlement for U.S. currency was up and running.

The second event was the London terrorist attack of July 7, 2005 that resulted in a partial shutdown of the London Stock Exchange (LSE). The LSE systems were unprepared to handle the flood of automatically generated trades intended to contain losses to distributed financial institutions. The LSE therefore asked member institutions to shut down their algorithmic "black box" trading systems, and created instead a fast market for non-binding, indicative pricing to make up the difference. Member institutions complied, shutting down their black box systems long enough for

the LSE systems to begin handling non-algorithmic trades properly.

These examples prove that highly complex, IT-based financial systems can be remarkably reliable. Problems in key centers such as New York or London were handled without global crisis. Backup systems on other continents were brought online to prevent financial disaster. In both cases, threats originated from outside the system, and the system responded well. The financial meltdown of 2008 was due to threats inside the system. What we now call toxic assets were in effect sleepers and Trojan horses, embedded in the system by the system's participants. Intrusion detection systems could not alert the risk managers because there were no intrusions. IT people had never imagined

that financial industry professionals in investment banks, brokerages, pension funds, and other organizations lacked the tools to treat simultaneous crises from operational, credit, and market risks through an integrated risk assessment. This was not the kind of crisis IT specialists planned for.

Liquidity Crisis

The collapse of Northern Rock, the U.K.'s fifth-largest bank, was the visible warning of the debacle to come. When Northern Rock was taken over by the British government in February 2008, no one considered the problems as related to IT. The crisis of Northern Rock was not big enough for that purpose. However, when Lehman Brothers failed on September 15, 2008 the role of IT in the debacle became clear. When Lehman Brothers faltered, financial institutions around the world were forced to reevaluate their risk exposure almost instantly. All of their IT systems were built on presumptions of an orderly flow of prudent business transactions; no one had imagined that the transactions themselves might be the problem. Lehman Brothers was an investment bank, an essential intermediary in global credit markets. Many banks had hundreds of millions of dollars queued up in payments to Lehman Brothers when the news broke. There were no IT routines in place to stop such transactions once they were initiated.

When it became clear that money was about to go into a black hole, the IT specialists in the banks did the only thing they could do: they pulled the plug on the IT infrastructure, thereby halting all operations. Banks around the world became risky partners simply because no one knew who was risky and who was not. All transactions were stopped and cash flow came to a halt. This was the dreaded "liquidity crisis" that is still being discussed widely. The only way banks could avoid sending good money after bad was to disconnect the IT systems from the global financial networks. Within hours, the lightning-fast global financial system had slowed to the speed of the pre-computer era. The effects were pervasive, hitting even the smallest financial institutions in the most remote corners of the Earth.

This crisis was not caused by IT, but an imbalance in IT infrastructure

> **It was not possible to assess risks of transactions as they occurred, so financial industry experts simply assumed the transactions were OK.**

played a major role in its origin. The problem was a discrepancy between two essential capabilities: the ability to execute transactions and the ability to comprehend the implications of the transactions being executed. IT departments within financial institutions were able to deliver "millisecond information flows" for real-time processing of transactions. However, they could not support counterparty credit risk calculations at speeds to match the transactions. It was not possible to assess risks of transactions as they occurred, so financial industry experts simply assumed the transactions were OK. A few experts making risky assumptions might be protected if the vast majority of experts are executing due diligence and evaluating risks carefully. The few benefit from the equivalent of "herd immunity" in vaccinations against disease. When all of the experts assume the transactions are OK, serious trouble can follow.

Credit risk calculations require a lot of work. The data for them must be gathered from many—sometimes several hundred—data warehouses. Data in such systems is often inconsistent and subject to quality control problems. During crises expert analysts often face absurdly simple but debilitating problems, such as trying to determine what the headers in their data sets mean, or trying to deduce which financial partners have provided given data. It seems difficult to believe that such data problems were allowed to continue even as IT sped up transactions to light speed. But as it often happens with IT, different parts of the IT ecology develop at different speeds.

ACM Transactions on Reconfigurable Technology and Systems

ACM Transactions on
Reconfigurable Technology
and Systems

SPECIAL EDITION ON THE 15TH INTERNATIONAL SYMPOSIUM ON FPGAs

This quarterly publication is a peer-reviewed and archival journal that covers reconfigurable technology, systems, and applications on reconfigurable computers. Topics include all levels of reconfigurable system abstractions and all aspects of reconfigurable technology including platforms, programming environments and application successes.

www.acm.org/trets
www.acm.org/subscribe

Association for Computing Machinery

Data Exchange Standardization

IT specialists might be surprised to learn that there are no standardized data exchange formats for traded asset classes. Some financial experts say it is difficult or even impossible to develop data exchange standards that cover all elements needed for sound risk assessments. The financial market is highly product driven, with extremely short development cycles. Standardization of data exchange formats might never catch up with what is being traded. But, as every seasoned IT professional realizes, such standardization must be *part of the product*. Otherwise, functions that require standardization, such as real-time counterparty credit risk calculation, might never catch up with the risks being taken. Legislators and regulators seeking to tame the financial markets must look at these matters systematically. Mandatory standardization of data exchange formats based on emerging schemes (for example, Financial product Markup Language, FpML) might have to be developed for different asset classes so that a common understanding of offerings and risks is possible with sufficient speed to accompany financial product offerings.

At present, financial firms cannot assess risk exposure in real time. They collect the necessary data and do the math during nighttime batch processing operations that can last hours. It would be a huge improvement if there were nothing more than systems to support initial heuristic risk assessment, but this might not be enough to avoid problems such as those of 2008. It might be necessary to slow transactions down until risk assessment can occur at the same speed the transactions occur.

Former chairman of the U.S. Federal Reserve Alan Greenspan has said that bank risk managers are more knowledgeable than government bank regulators, and that regulators cannot "lean against the wind" to dampen economic swings. This might be correct, but bank risk managers need the right systems to do their jobs. The IT systems used to support assessment of counterparty credit risk are not as mature as transaction systems, especially for integrated assessment of operational, credit, and market risks. Individual desks at an institu-

> **It might be necessary to slow transactions down until risk assessment can occur at the same speed the transactions occur.**

tion might do a good job at evaluating risks for their department, but they lack the global enterprise perspective that is vital to a global financial industry. This must change. Financial institutions are looking for improvements to data management, risk evaluation algorithms, and simulation systems, not because they are forced to do so by regulation, but because these are essential to their survival. The crisis has shaken confidence in the ability of IT systems to support the risk assessment at the heart of financial system operation, regulation, and market transparency. However, only by improving IT systems to support such assessment can the global financial industry move forward.

Perhaps financial regulators should not lean against the wind, but improved IT systems might play a vital role by helping bank risk managers do their jobs more effectively. IT professionals, working closely with colleagues from other business departments, can create industrywide, canonical data exchange standards to help with management of risk by improving data quality across organizations and borders. In this way, IT might lean against the wind of threats to global financial markets by enabling mature and embedded analytics that must influence decisions in financial institutions. Pulling the plug was a poor response to the crisis of 2008; the next time it might not work at all. Ⓒ

Roman Beck (rbeck@wiwi.uni-frankfurt.de) is an assistant professor with the E-Finance Laboratory in the Department for Economics and Business Administration at Goethe University Frankfurt, Germany.