MI FORUM

ROCKET MAN

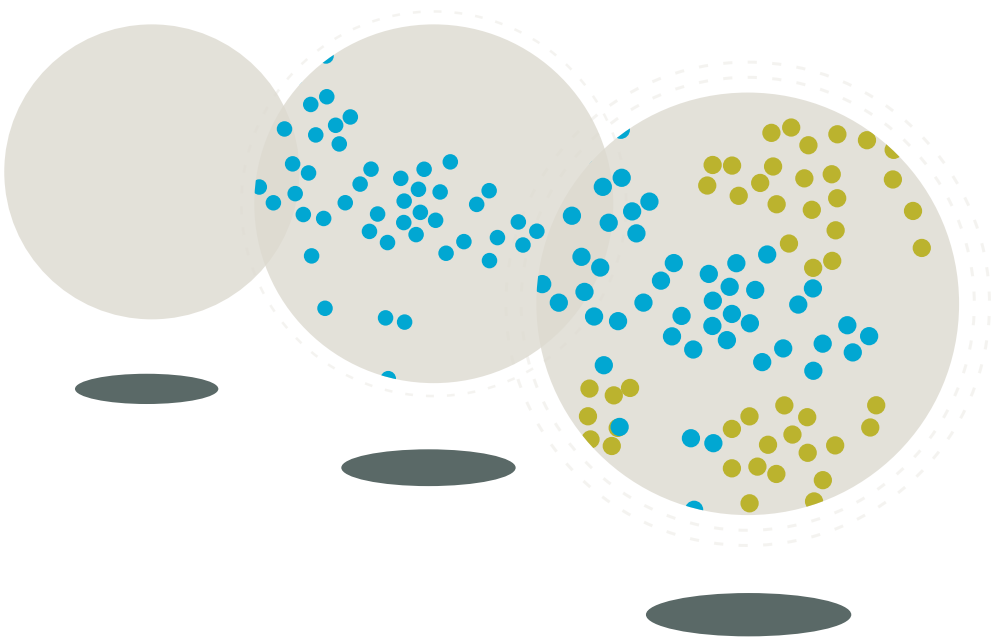
The CSD chief who thinks regulators have something useful to say

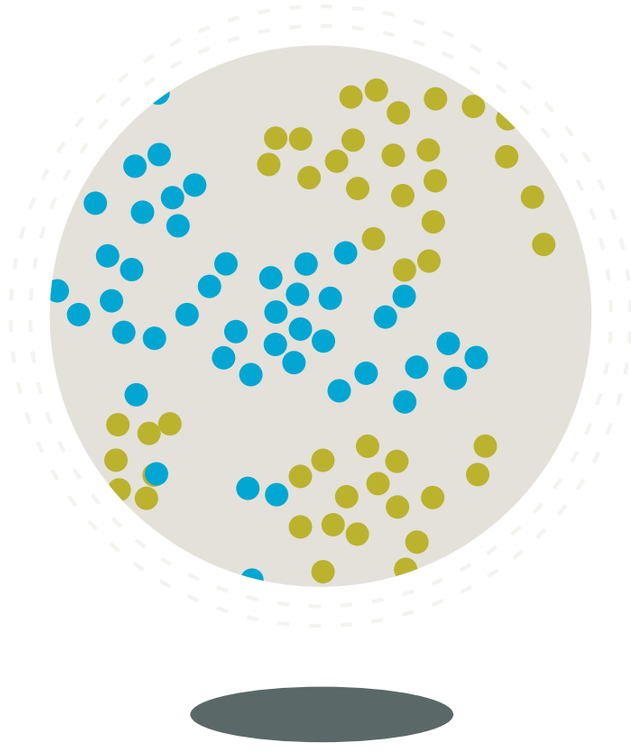
CYBER CITADEL

How to build a third line of defence against cyber-criminals

MARKET INFRASTRUCTURES:

IN PURSUIT OF THE FUTURE





Market Infrastructures Forum magazine / Issue 4

Editor
Dominic Hobson
dominichobson@dominichobson.com

Head of Market Infrastructures, SWIFT
Juliette Kennel
juliette.kennel@swift.com

Design
Bim Hjortronsteen
bimhjortronsteen@gmail.com

Publisher
SWIFT
Avenue Adèle 1
B-1310 La Hulpe
Tel: +32 2 655 31 11
Fax: +32 2 655 32 26
SWIFT BIC: SWHQ BE BB
http://www.swift.com/

Contents

Introduction:

Market infrastructures are terra-forming the future

The term infrastructure was once synonymous with the foundations of an economy. The foundational character of infrastructures means that they have always had a profound effect on the behaviour of the participants that make up the industries that use them. Certainly the banks, brokers and fund managers that make up the payments and securities industries expect the financial market infrastructures (FMIs) that underpin their commercial activities to be unfailing, and unimpeachable.

Yet one of the many effects of the increasing power and falling price of digital technology is to transform the potential of FMIs. As recently as a decade ago, when TARGET2-Securities (T2S) was conceived, our thinking about FMIs was conditioned by the costs of technology. Given these high costs, the building of an FMI had to be funded collectively. Moreover, the only way to mitigate the concern of users that infrastructural monopolies would exploit their position by charging higher prices for the same or even less work was for FMIs to be owned by a public authority or owned and governed by their users.

The digital opportunity for FMIs

The cheap, powerful and widely available digital technology of today has fundamentally altered the terms of that equation. By reducing the marginal cost of processing a transaction effectively to zero, digital technology creates an opportunity for FMIs to break with their past. Instead of being regulated as monopolies, they can become competitors themselves, and enablers of competition between others. Just as the Internet has enabled more companies to compete to sell goods all over the world, so can digitally empowered FMIs enable established businesses and new entrants to compete to sell financial transfer and intermediation services all over the world.

Many of those businesses will provide services we cannot even conceive of today. Digitisation is giving FMIs the power not simply to transform the landscape but – to coin a metaphor from physics - to terraform entirely new planets which can support unprecedented forms of financial and commercial life. In this transformed financial universe, FMIs will become the shared means to many ends. In the payments and securities industries, multiple transactions which entail the delivery of an asset against cash payment in digital form - such as foreign currency bargains or the sale and purchase of securities or mutual funds – are already being supported by FMIs. In future the range of transactions they support will multiply enormously.

How the digital opportunities will unfold, only time will tell. But some of the new opportunities are already obvious. Our round table discussion (p.66) explores how central securities depositories (CSDs) in Asia are looking to support banks and fund managers in the development of a regional mutual fund market, driven by distribution passports, with efficient post-trade services. This matches similar developments in the European mutual fund markets. Likewise, Inge van Dijk (p.92) describes how Dutch payments systems are working with retailers and banks to develop instant payment services that exploit the power of digital technology.

Terra-forming is the engineering of a barren planet to create an environment where life can prosper. It is an apt metaphor for the deliberate re-shaping of the infrastructural landscape we have inherited to create a safer environment for existing business and to encourage new forms of commercial life to prosper.

The systemic constraint on FMIs

The evolution of this new, digital eco-system will be driven by interactions between FMIs and their users, of both the collaborative and the commercial kind. Eddie Astanin (p.10) says that NDS is already experimenting with distributed ledger technology (DLT) to test whether it can make those interactions still cheaper and more efficient in, for example, the fields of corporate actions processing and proxy voting. However, as Virginie O'Shea points out in her article (p.86),

the speed of adoption of DLT by FMIs is bound to be tempered by the systemic importance of the services they supply. FMIs cannot embrace the digital future, no matter how exciting, if there is any chance that this could jeopardise business-as-usual activity.

This dilemma is at an acute stage in real-time retail payments (RTP), where instantaneous payments systems are now being developed, which banks will be able to "overlay" with innovative payment services. As Lisa Lansdowne-Higgins writes (p.80), the banks, clearing and settlement mechanisms (CSMs) and regulators that are driving progress towards RTP are debating whether it is safer to adapt existing infrastructures, or to build new systems, and whether it is more prudent to aim for a single platform or to maintain multiple payment systems.

In Canada, regulators have already decided to aim at a single platform for all forms of payment, convinced that a single, open utility can promote competition in the payments industry more effectively than multiple platforms, each with their own rules and guidelines, governance and access models, and each charging a separate membership fee. In the United Kingdom, an expert body created by the Payment Systems Regulator (PSR) has called for consolidation of three existing CSMs: Bacs; the Cheque and Credit Clearing Company; and Faster Payments, as the foundation of a new payments platform that will create a safer environment for market infrastructures to provide established and innovative services to their customers.

Standards underpin inter-operability

In digital interactions, the inability to exchange information in a common language is a significant source of avoidable operational cost, so the widening use of the ISO 20022 standard will ensure that the cost of market interactions will continue to fall. Soon, close to 200 FMIs – including T2S and, eventually, the TARGET2 cash payments system also operated by the European Central Bank (ECB) – will be able to communicate with their users via ISO 20022 messages. This is already reducing the cost of connecting to multiple different market infrastructures.

But there is another sense in which ISO 20022 will make an even greater contribution. This is interactions between FMIs, or what the payments and securities industry refers to as "inter-operability." In their contributions to this issue, Harry Newman (p.58) and Jeremy Light (p.62) agree that the ability to exchange information through a common standard is essential if domestic payments systems are to inter-operate, especially across borders. The remaining obstacles to such harmonisation are multiple and far from negligible, and FMIs must address them if they are to remain relevant in a world being turned upside down by economic and regulatory pressures, as well as the cost-reducing powers of digital communication and computation.

FMIs can still cut costs by creating synergies

The rising cost of capital and liquidity, and especially of un-collateralised borrowing, is tightening the links between asset classes. The ECB has already announced that it will merge its high value payments system (TARGET2) with its securities settlement system (T2S) in 2020. There could be no clearer signal of the synergies between cash, securities and collateral. As Yves Mersch points out in his article (p.24), the closer integration of the various components of the financial market infrastructure of the Eurosystem will help to enhance the safety and efficiency of payments, securities and derivatives by making it cheaper and easier to access liquidity, credit and collateral.

In a global marketplace in which virtually every equity or bond is potentially eligible collateral to secure central or commercial bank money, FMIs must find ways to cut the costs of moving assets between their account-holders, and on a truly global canvas. Inevitably, the business case for infrastructural transformations of this kind is complicated by the current diversion of technology budgets into projects to comply with regulatory demands. But this is poised to change, and not just because the long list of post-crisis

regulations affecting the industry may now be coming to an end.

As Natasha de Téran recounts in her article (p.50) about the proposed European Capital Markets Union (CMU), regulators are now alive to the possibility that some of the regulatory measures taken since 2007-08 are proving counter-productive to closer integration of markets. She adds that the framers of the CMU also recognise that many of the most persistent barriers to integration – on which the business case for links between FMIs ultimately rests - are not infrastructural at all, but legal, fiscal and regulatory. All of these barriers are under the control of the authorities.

FMIs can help defeat cyber-crime

One barrier to progress in integration that is not under the control of anybody, yet is becoming steadily more important, is cyber-crime. As Yves Poullet writes in his contribution (p.39), the negative potential of cyber-threats is destructive enough to overwhelm all of the benefits of the digital revolution. In facing up to that peril, FMIs understand that they are particularly at risk, not least because failure really is not an option, given their responsibility to ensure secure settlement of critical transactions. The recommendation by CPMI-IOSCO that FMIs adopt a two-hour downtime limit is an accurate measure of the critical importance of FMIs to entire financial systems.

Richard Dzina suggests (p.32) that FMIs must now consider investing in a third level of resiliency and security. As Stephen Gilderdale points out (p.42), FMIs are natural inheritors of prime responsibility for cyber-security, since they came into existence to reduce operational risks and costs. Indeed, the SWIFT Customer Security Programme is already helping its users address mounting cyber-threats, by setting a security baseline for SWIFT-related customer business, deploying a third party identity assurance framework, improving transaction pattern detection, and through increased sharing of cyber-security intelligence.

As John Hagon (p.38) and Trevor Spanner (p.40) note, other FMIs are equally involved in the sharing of intelligence about cyber-threats. It is work to which FMIs, with their long history of neutrality and mutual ownership and governance, are well-suited. They are instinctive collaborators as well as competitors, who share experience and information naturally. This magazine - whose content is created entirely by market practitioners - is evidence of that.

That collegial spirit is now being put to the ultimate test by the tempting opportunities created by the digital revolution. Each FMI will strike its own balance between the need to innovate to remain relevant and the obligation to provide a reliable underpinning to the work of others. But, as Nadine Limbourg and Isabelle Olivier point out in their contribution (p.44), this is a familiar challenge for FMIs. They are used to doing the hard and unglamorous work of translating strategic visions into services that actually work.

In this sense, FMIs are the real agents of transformation in our industry. They are, to stick with the metaphor, terra-forming a wholly new landscape. The pace of that transformation is undeniably accelerating, which is making it harder for all of us to keep up. In fact, developments are now proceeding so fast that MI Forum magazine is not going to wait until Sibos Toronto to update its readers. We will be publishing online as well from October this year at www.swift.com/your-needs/market-infrastructures, where we look forward to reading your comments and contributions just as much as we hope you look forward to reading ours.

Juliette Kennel

Head of Market Infrastructures, SWIFT
juliette.kennel@swift.com

Rocket man

MI FORUM 2016 | GENEVA

In his appetite for innovation, Eddie Astanin cuts an unusual figure among the leadership of financial market infrastructures. But in his conviction of the possibility of positive relations between regulators and regulated, his willingness to learn from and apply the experience of others, and in his belief that extended global networks of CSDs can be built without amalgamation, the CEO of the Russian CSD paints a vision of the future of infrastructure that is utterly convincing.

Eddie Astanin is a rocket scientist. This may not be quite the compliment it was in the years before the financial crisis, when physicists blended mathematics, finance and computing power to create what Warren Buffett dubbed "financial weapons of mass destruction."

But after graduating in 1984 from the Space Academy in Leningrad, where he specialised in the mathematical modelling of ballistics - the movement of objects through space – the 22-year-old Astanin began his career as a research mathematician attached to the military space institute. By the time he left a decade later, Eddie Astanin had a doctorate in ballistics.

"It was a good grounding for my future career in the financial services industry," he jokes. Now the chairman of the executive board of National Settlement Depository (NSD) in Moscow, Eddie Astanin can look back on a career trajectory at least as steep as that of a rocket. For he joined National Depository Centre (NDC), as the Russian central securities depository (CSD) was then known, as recently as December 2004.

Closing the gap between front and back

His invitation to become the chief operating officer (COO) of the NDC – set up in 1997 by the Bank of Russia, Moscow Interbank Currency Exchange (MICEX) and the domestic and foreign custodian banks - came from Andrei Kozlov, then the first deputy chairman of the Bank of Russia.

"He was the outstanding leader and driver of the process of development of the financial markets

in Russia," says Astanin. "He had an absolutely clear vision of how the financial markets and the banking industry should develop. It was a tremendous honour for me to be invited by him to become the COO of the NDC."

The brief Kozlov gave to Astanin and the NDC team was to build a new technology platform for the CSD. It was sorely needed. At the time, the platforms for trading bonds and equities had outstripped the capacity of the post-trade systems to settle transactions safely and efficiently. "NDC needed to improve the scalability and reliability of its systems," explains Astanin. "In terms of efficiency, it had to catch up with the trading platforms."

Kozlov knew he could trust Astanin to close the gap, because he had seen him develop a platform for the government bond market already. After joining the Moscow Exchange, the parent company of the NDC, Astanin had overseen the development and installation of a national bond trading platform.

The new platform was adopted not only by Moscow Exchange, but by the independent regional exchanges that were in the 1990s active in several of the largest cities in Russia, from St Petersburg to Vladivostok. Astanin even wrote the rulebook for the trading firms that used it. Inevitably, he also had to take an interest in how trades settled, so by the time he joined NDC in 2004 he had plenty of direct experience of the role and capabilities of the CSD.

"The platform of the NDC was obviously inter-connected with the trading platform of Moscow Exchange," explains Astanin. "That was one of the reasons Andrei Kozlov trusted me. He paid a lot of attention to post-trade, and the revitalisation of NDC was very much his project." Sadly, Kozlov did not live to see the launch of the new platform but, with the help of consultants from both Accenture and TCS, it went live in 2008.

In 2009 Astanin had been appointed as chief executive of NDC. In April 2009 the NDC had transformed itself from a not-for-profit into a joint stock company, as the prelude to a merger with the MICEX Settlement House (MICEX SH), then still wholly owned by MICEX. It was the initiative of the Bank of Russia as a main stakeholder of Moscow Exchange. The aim was to create a single CSD for Russia.

Changing the culture of NSD

When MICEX merged in December 2011 with the rival Russian Trading System (RTS) platform to create the Moscow Exchange Group of today, the ambition to create a single CSD was finally fulfilled. In 2012 NSD absorbed not only the RTS Settlement Chamber but the Depository Clearing Company (DCC), which provided CSD services to firms trading on RTS. "It was my first experience of mergers and acquisitions, and I am proud that it was a success, because we know from the statistics that 75 per cent of mergers fail," says Astanin.

By November 2012, Eddie Astanin was master of a single CSD for all Russian securities. With the integration of four post-trade utilities complete, the next task was to devise a growth strategy for the merged entities.

As it happens, strategy-making was not the most difficult task. "It was much harder to change the corporate culture," recalls Astanin. "It meant hiring from local and foreign companies new people with the right knowledge, skills and experience, and firing

the people who still clung to a monopolistic rather than a client-orientated culture."

It is a measure of his stature, not only within Moscow Exchange Group but within the wider financial marketplace and the regulatory environment, that Astanin was able to accomplish such sweeping changes. This owed a great deal to his prior experience in the government bond markets. By the time he assumed leadership of the new NSD in 2010, he had already worked with colleagues, bankers and regulators in Moscow for a decade and a half. They knew him, and he knew them.

The unexpected regulatory lesson of August 1998

Being architect of the government bond trading platform also gave Astanin a ring-side seat at the event which shaped everything that has happened in the Russian financial markets since the turn of the century: the crisis of 17 August 1998, when the currency was devalued, and the country defaulted on its debt.

"I was in the centre of the storm," recalls Astanin. "I remember the morning of the day we got the order from the Bank of Russia to stop trading." But he extracted from the experience something that delegates to the May 2015 Cancun meeting of the World Forum of CSDs – a body Astanin headed for two years – were surprised to learn. Asked what single factor was most helpful to the development of CSDs, and which was most unhelpful, Astanin replied unhesitatingly: "Regulation, and regulation."

What he meant was that the nature of the interaction between regulators and regulated can accelerate or obstruct the progress of development and reform, particularly in the

"The nature of the interaction between regulators and regulated can accelerate or obstruct the progress of development and reform, particularly in the wake of a crisis."

wake of a crisis. Astanin reckons it took Russian market participants at least five years to recover from the shock of 1998. But he believes it would have taken even longer if the Bank of Russia and the Ministry of Finance had not made serious efforts to re-write the regulations in ways that addressed the concerns of the marketplace.

Astanin played his part in one of the crucial reforms of the government bond market that followed: the introduction in 2001 of a repo market. This had the predictable effect of enhancing liquidity in Russian government bonds, but it also provided a stable source of central bank funding for privately owned banks. Fittingly, one of the responsibilities of NSD today is the provision of tri-party collateral management services to banks raising central bank money in the repo market.

Recognition of the importance of repos to government bond markets illustrated the willingness of Astanin and his regulatory counterparts to learn from the experience of developed markets. “In some countries, it took decades to develop bond markets, trading platforms, and regulations,” says Astanin. “We used the experience of others not just to avoid mistakes, but to jump from a sketch to a fully dematerialised marketplace in one leap.”

Innovating instead of talking

That willingness to learn, and to innovate, has become an ingrained aspect of the corporate culture of NSD under Eddie Astanin. Nothing illustrates it as well as the fact that it took NSD just five months to initiate and test a blockchain technology to handle corporate actions and e-proxy voting. It was one of four potential use cases identified by a specialist group set up by Astanin as recently as November 2015.

To deliver a workable prototype, NSD hired a group of London-based developers at bitcoin platform Digital Securities Exchange (DSX). “We can already process 80 transactions a second, but our initial goal is to raise that to 300 transactions a second, and we know we can achieve it,” says Astanin. “On the basis of this experience alone, I can say that blockchain technology definitely has a future - maybe not in the core business of the CSDs, but certainly in associated areas.”

Among the “associated areas” identified by NSD as ripe for reform by distributed ledger technology are its trade repository services. As it happens, the trade repository, originally designed to bring Russia into line with the G20 pledge to ensure all clearable OTC derivatives are reported, has already increased its traffic from zero at the start in 2013 to 450,000 submissions from 1,173 financial institutions in 2015. Corporates will start reporting their trades to the repository later this year.

That alone makes the trade repository one of the main axes of growth at NSD. Another is tri-party collateral management. “It has proved a very successful project,” says Astanin. “Now more than 200 banks are using the service. Practically all of the major international custodian banks active in Russia use us to provide them with a government bond repo service that enables their clients to raise finance not just in rubles but in euro and US dollars as well.”

Custodians can now also offer clients trading Russian securities settlement in central bank money, since NSD has introduced an

CIPS

Cross-border Interbank Payment System

As important financial infrastructure, the Cross-border Interbank Payment System (“CIPS” hereinafter) provides clearing and payment services for financial institutions in the cross-border RMB and offshore RMB business. The establishment of CIPS is carried out in two phases, the first phase is to facilitate processing of cross-border RMB business and to support settlement of cross-border trade in goods and services, cross-border direct investment, cross-border financing and cross-border individual remittance.

The operator takes full charge of operation and maintenance of CIPS, service rendering to participants and business expansion of CIPS under supervision and administration of the People’s Bank of China. The operator will gradually improve system features as required by market demands, enhance its internal management and increase its clearing efficiency and competitiveness.

China International Payment Service Corp. (“the operator” hereinafter), a corporate entity, was incorporated on 31st July, 2015 in Shanghai with the approval of the People’s Bank of China.

- Settlement of Cross-border Trade
- Settlement of Cross-border Direct Investment
- Settlement of Cross-border Financing
- Settlement of Cross-border Individual Remittance
- Other Settlements

Website: http://www.cips.com.cn E-mail: cips@cips.com.cn

automated clearing house (ACH) service that connects banks directly to the real time gross settlement system (RTGS) of the Bank of Russia. “We have become the biggest payment system in the Russian financial market after the Bank of Russia,” says Astanin. “We are facilitating the settlement of payments worth more than 300 trillion rubles a year.”

Settlement in central bank money represents a major advance in risk mitigation for investors in the Russian securities markets. Until it introduced the service last year, NSD could settle transactions in commercial bank money only.

How to become a data vendor

An even more popular idea with the banks is the assumption by NSD of responsibility for the accuracy of corporate actions data and other information about securities. From 1 July this year, under legislation passed in the summer of 2015, NSD became the sole official source of information about issuers, their securities, the identification codes and prices of those securities, and the entitlements attached to them. NSD also provides a valuation tool for investors in illiquid instruments.

Astanin sees the valuation tool as important, since it exemplifies the ability of NSD to turn Big Data into information. He promises customised analytical services to clients, and points to the success of NSD - assisted by mathematicians at the Russian Academy of Mathematics - in reducing the time taken by its tri-party engine to calculate collateral calls from 300 seconds to just four. “It is an example of how we are able to use Big Data,” says Astanin.

Leading the world into ISO 20022

Importantly, all of the information is couched in the ISO 20022 standard. With the new payments system also adopting the ISO 20022 standard, NSD has become a world leader in terms of compliance with the new standard.[1] “ISO 20022 is invaluable not just for CSDs, but for issuers, registrars, custodians, payments banks and central banks,” says Astanin. “In fact, the Bank of Russia is keen for us to standardise communications between market participants beyond the banking sector, including insurance companies, pension funds and corporates. We have plenty of support from our regulator on standardisation.”

He reckons the ISO 20022 standard will help achieve an astonishingly ambitious goal he has set: to raise the proportion of securities messages carried on the SWIFT network from less than a tenth of the overall SWIFT traffic generated by NSD to at least half. Regulatory enthusiasm for ISO 20022 is also a further reminder of the importance Astanin attaches to positive dialogue between the regulators and the regulated.

“In Russia, we have helpful co-operation between regulators and the infrastructure,” he says. “We have the willingness, and the opportunities, to develop our infrastructure without wasting time and energy on personal or political battles. That does not mean we do not have strong debates from time to time.”

Building a global CSD network

One of those strong debates was over whether or not it was sensible to allow foreign banks to open nominee accounts at NSD. It took nearly a year to resolve. But when the first foreign nominee accounts were finally opened for Clearstream and Euroclear, the consequent rise in the price of government bonds knocked 150 basis points off the average yields of Russian government debt. “The results proved we were right to argue for foreign nominee accounts to be allowed,” says Astanin.

In fact, the success of the links with Clearstream and Euroclear has encouraged him to seek similar arrangements with the CSDs of Asia. Memorandums of understanding are now in place with the CSDs of China, Hong Kong, Japan, India and South Korea. “The idea behind them is to provide direct access to these markets for Russian investors, and foreign investors with direct links to the Russian markets,” explains Astanin. “We know there is a real appetite from both sets of investors for links of this kind.”

In April this year he was in China, to lay the foundations for links with the Chinese CSDs. “Technically, the links are not difficult for us to set up,” says Astanin. “But it will take some time to turn the proposed link into reality. For the Chinese regulators, ten years is no time at all. We respect Chinese culture, so we do not want to push forward too aggressively. We prefer an evolutionary approach to a revolutionary one.”

Patience is an unexpected virtue in a man who has orchestrated change at a fierce pace in the 20-odd years he has spent in financial markets. Perhaps all rocket scientists think faster and see further than most people, but in his time at what is now Moscow Exchange Group, Astanin has created an electronic bond market, merged multiple CSDs into one, reinvented the internal culture of the merged entities, built a trade repository, and gone further and faster than any CSD in the world in reforming corporate

“The idea is to provide direct access to these markets for Russian investors, and foreign investors with direct links to the Russian markets. We know there is a real appetite from both sets of investors for links of this kind.”

- Eddie Astanin,
CEO of the Russian CSD

1 See “The challenges and rewards of an ISO 20022 pioneer,” in MI Forum magazine, Issue No. 3, 2015, pages 22-28.

actions data and processes, introducing e-proxy voting, and driving adoption of the ISO 2022 standard. Under his leadership, NSD is now deep into Big Data and blockchain projects.

"At the end of the 1980s, Russia had its break with history, creating a palimpsest on which people such as Eddie Astanin could script a future free of legacy interests, systems and clients."

- Eddie Astanin,
CEO of the Russian CSD

History creates shortcuts to the future

In short, the NSD of Eddie Astanin has become a world leader in infrastructural reform and innovation. Astanin is the first to admit that the external environment helped. At the end of the 1980s, Russia had its break with history, creating a palimpsest on which people such as Eddie Astanin could script a future free of legacy interests, systems and clients. But Astanin himself also lived that break, and is mindful that factors other than historical chance were at work.

Born in Moscow when it was still the capital of the Soviet Union, Astanin was raised at Baikonur in Kazakhstan, where his father worked at the cosmodrome. At the time, the Russian space programme was run by the military, and his father was a military space engineer as well as a mathematician engaged in the development of ICBMs armed with nuclear warheads. When he entered the Space Academy in what was then Leningrad in 1979, Eddie Astanin expected to follow exactly the same career path as his father.

The collapse of the Soviet Union in the early 1990s put paid to that expectation. By then, Astanin was married to Alexandra – though she too was raised in Baikonur, because her father was also a military space engineer, they did not actually meet until they were both in Leningrad. Now they have two children and two grandsons. "It was a difficult time, with the Soviet Union breaking up into different countries, and I had to earn money for my family," he says. "So I decided to leave the armed services, and get a financial education."

Astanin enrolled at the Financial Academy in Moscow. With his deep knowledge of mathematics, the course was not difficult for him, but it did take two years. It was after graduating in 1994 that he joined MICEX. His first role – it is an apt measure of the times – was to run the entire department responsible for the electronic trading of government bonds. "Maybe I was a little bit lucky, but it was a good time to join the company," says Astanin. "Everybody had an opportunity to find their personal niche, from which to build their career."

Together, regulators and regulated make things happen

But he argues that neither his career nor the subsequent development of the Moscow Exchange Group owed much to the initial conditions. Astanin reckons it was entirely possible for the break with history to have propelled the Russian financial markets down a cul-de-sac. What averted that possibility, he reiterates, is the willingness of the individuals at both the regulatory agencies and Moscow Exchange Group to work together to effect change.

"Our regulator – the Bank of Russia – and the Ministry of Finance are progressive," explains Astanin. "They want to develop our financial markets infrastructure. They understand the strategic benefits of it. Likewise, the management of the Moscow Exchange Group has a strategic vision. We want to change our industry. We prefer a leadership style of management, because we want to change the company, and change the environment in which we operate. In co-operation with the regulator, change is much easier to accomplish."

Change certainly holds no terrors for a man whose life and career were overturned by a disruption of world-historical proportions. Indeed, Eddie Astanin sees nothing but opportunity for CSDs in the much-discussed technological disruptions of today. A trip to Silicon Valley with fellow members of the SWIFT Board encouraged him in his conviction that blockchain is just one of a triad of developments – the others are Big Data and the Cloud – driven by the fall in the cost-power ratio of digital computing technologies.

New opportunities are opening up for CSDs

"FinTech is a huge threat to financial intermediaries," says Astanin. "Are CSDs a victim of the same future? I am not so sure. I think FinTech means more opportunities than threats for CSDs. We have something similar to what PayPal and Visa have: a crucial role at the centre of a network. NSD is already a centralised platform for different types of activity, such as settlement, collateral management and the storage of information about transactions in a data repository. Scaling our platform up, and giving end-users access to it – that is where the future of the CSD industry lies. We can make it much easier and safer for customers to use their digital gadgets to get information as well as complete transactions."

His vision of the future of CSDs on the global scale is equally vivid. "We do not face competition in the services we provide in our national markets, but CSDs are nodes in a global network," explains Astanin. "Every financial centre is competing on that network for the limited resources of global investors, and CSDs help them do that. But

CSDs are and will remain national institutions, especially in their role as issuer CSDs. The best way to develop CSDs across borders is not to merge them, but to connect them via bi-lateral links between investor CSDs. Those links will not only allow users of CSDs to access other markets at lower cost, but create much less resistance at the national level, and so allow a global network of CSDs to evolve more smoothly."

The effectiveness of those bi-lateral links ultimately depends on the ability of CSDs to agree on standardised communication protocols, and to harmonise their working practices. Eddie Astanin knows this. While he yields to no one in his belief in the beneficent power of competition ("Competition is good - it brings a real edge to our development"), he argues that friction-less networks are more powerful still. In fact, the main reason he agreed to chair the World Forum of CSDs for two years was his belief that standardisation and harmonisation could create a genuinely valuable global network of CSDs.

"There are more and more common points of integration between CSDs," says Astanin. "CSDs are becoming increasingly important elements in the global financial network." In the meantime, the culture of innovation he has instilled at NSD is taking the Russian CSD in some interesting directions.

The unanswered question is whether Eddie Astanin can maintain the momentum. He thinks he can. "Every company has the opportunity to use its resources to innovate, and there are plenty of companies which are more successful than NSD at doing that," concludes Astanin. "They are the benchmark for us. I am confident we can compete with them. Big companies may have more resources than us, but we are more flexible."

"Every company has the opportunity to use its resources to innovate. Big companies may have more resources than us, but we are more flexible."

- Eddie Astanin,
CEO of the Russian CSD

The future at your fingertips – the European market infrastructure of tomorrow

Vision is the art of seeing what is invisible to others.

- Jonathan Swift

MI FORUM 2016 | GENEVA

The market infrastructure of the Eurosystem is working well, but further measures are needed to deepen market integration, increase operational efficiency and address the challenges of new technology. The three priorities identified by the Eurosystem, writes Yves Mersch, a Member of the Executive Board of the European Central Bank (ECB), are the consolidation of its payments (TARGET2) and securities (T2S) settlement services, the creation of pan-European Instant Payments, and the development of a common collateral management system.

Like plumbing, electricity and telecommunications, a financial market infrastructure is at its best when largely invisible. Like plumbing, electricity and telecommunications, it spans not only the physical applications but also the operating procedures, management practices and development policies that interact with market and societal demands. And like plumbing, electricity and telecommunications, it needs constant care, maintenance and development to keep pace with technological advances and the changing needs of users.

The reason why this text seeks to shift the financial market infrastructure of the Eurosystem from "invisibility" and place it in the limelight is that, to ensure its smooth functioning now and in the future, further efforts are needed to bring about deeper integration and increase efficiency. Additionally, the challenges emerging from technological innovation and their potential future use in the financial market infrastructure will have to be addressed.

From strategic reflection to strategic action

One year ago, the Eurosystem put forward some initial reflections on the strategy for the future development of its market infrastructure.

These strategic reflections are geared towards keeping pace with market developments and deepening European market integration in line with the Capital Markets Union (CMU) initiative launched by the European Commission.[1] They are also aimed at reaping efficiency gains through technological consolidation and reviewing the service portfolio against changing business needs and new technologies.

In response to these strategic reflections, the Eurosystem has developed three key action points. The first is the consolidation of TARGET2 and TARGET2-Securities (T2S); the second is instant payments; and the third is a common collateral management system for the Eurosystem.

For all three action points, the goal of the Eurosystem is to work in close co-operation with the market in order to benefit from its knowledge and experience as well as to ensure that the future financial market infrastructure of Europe fully meets the needs of users.

1 See Natasha de Téran, "The CMU promises a joined-up approach to integrating EU capital markets," **p.50**.

> **"Retail payments should be made available by service providers in the same way as any other digital content – 24/7, instantaneously and across borders."**
>
> **- Yves Mersch, Member of the Executive Board of the European Central Bank (ECB)**

The consolidation of TARGET2 and T2S

TARGET2 and T2S offer similar services in the area of payments and securities settlement. But as they were developed at different points in time, they operate on separate platforms and use different technical solutions and environments. Hence, it is logical, with the go-live of T2S, to seek to draw on the synergies between both systems.

Consolidating the technical and functional components of TARGET2 and T2S services will allow TARGET2 to benefit from some of the state-of-the-art features of T2S, such as the implementation of ISO 20022 standards. It will also allow for further improvement of cyber-resilience and the establishment of a single access channel for market participants to connect to the Eurosystem market infrastructure. Last but not least, it could also lead to more cost-efficiency both in the running and further enhancement of both systems.

To identify market needs and find the most appropriate solutions to address them, the Eurosystem released a consultative report on real-time gross settlement (RTGS) services in February 2016.[2] TARGET2 users and other interested stakeholders were invited to share their views on the future provision of RTGS services.

More than 120 institutions from 22 European countries sent their feedback, welcoming the opportunity to contribute their ideas to the plans of the Eurosystem to review its RTGS functionalities and services. Overall, the respondents showed strong support for the Eurosystem plan to consolidate the TARGET2 and T2S platforms as a means of achieving greater efficiency and supporting innovation.

Respondents to the consultation were in favour of the idea of a harmonised interface and a single gateway to the payment and securities settlement services provided by the Eurosystem. They expect it to bring clear benefits in terms of cost savings and simplification for end-users. Many respondents provided positive feedback on the idea of having multi-currency RTGS services.

The market also provided positive feedback on operating hours possibly being extended, liquidity management tools and data analysis services. This feedback is being further assessed to establish the extent to which more sophisticated services in the area of liquidity management, business intelligence and compliance with regulations are required.

Instant payments

In the retail payments domain, the emergence of instant payments in a number of countries around the world reflects the expectation of users that retail payments should be made available by service providers in the same way as any other digital content – 24/7, instantaneously and across borders. In Europe, instant payment solutions have emerged or are being developed in a number of national markets. However, no instant payment solution is available yet for the euro at pan-European level.

For the Eurosystem, the biggest challenge of digitalisation in the payments industry is to ensure that the introduction of innovative payment products and services does not reintroduce fragmentation into the European market. That is why the Eurosystem, in conjunction with the European legislator and the Euro Retail Payments Board (ERPB), is attempting to foster the development and implementation of pan-European solutions.

In order to ensure that at least one pan-European instant payment solution for euro that is open to any payment service provider in the European Union (EU) becomes available, the ERPB called on the market to develop a pan-European scheme for instant payments based on the Single Euro Payments Area (SEPA) credit transfer. The scheme is due to be implemented by November 2017. By that time, end-user solutions for instant payments in euro should be made available at pan-European level by payment service providers.

This means that by November 2017 the European financial market infrastructure has to be ready to clear and settle instant payments on a pan-European scale. The Eurosystem has steered the work of the industry to identify the business requirements for settlement and risk mitigation, clarify the access criteria for payment service providers and other infrastructures, and define the elements for a framework for automated clearing house (ACH) inter-operability.

To meet the objective of achieving pan-European reach for instant payments without obliging payment service providers to participate in more than one ACH, the industry signalled its willingness to set up a number of links between ACHs. The setting-up of links is subject to a commercial decision by the ACHs and does not come without challenges.

The Eurosystem is prepared to support industry efforts to provide a pan-European reach for instant payments. The settlement of instant payments in euro between different ACHs could

2 European Central Bank, *Eurosystem's vision for the future of Europe's financial market infrastructure, RTGS services – consultative report*, February 2016.

be achieved by enhancing one of the existing ancillary system interface models in TARGET2.

At the same time, the Eurosystem will study the feasibility of establishing a more centralised real-time settlement service of pan-European instant payments in central bank money. Such a centralised service could guarantee pan-European reachability for instant payments; give users the possibility to use their credit lines stemming from their collateralised positions in TARGET2; eliminate credit risk, thus leading the way to faster and more efficient settlement; and give market players more choice.

A common Eurosystem collateral management system

As the banking and financial markets of the euro area become increasingly integrated, demand for more efficient collateral management arrangements is increasing. To date, collateral management in the Eurosystem is somewhat fragmented, as each national central bank has its own procedures and systems in place. As a consequence, some collateral management services are not provided in a fully harmonised manner.

This is something the Eurosystem seeks to address. As we look to the future, the Eurosystem will drive harmonisation forwards, particularly regarding Eurosystem operations for the mobilisation of marketable assets, as well as the handling procedures for non-marketable assets. There may even be a business case for a common Eurosystem collateral management system, since the market is becoming increasingly reliant on cross-border collateral flows for secured funding and treasury management operations.

A common governance framework

Settlement of payment transactions in central bank money, securities settlement and collateral management are the three cornerstones of the market infrastructure of the Eurosystem. Between these three cornerstones, services for the provision of liquidity, the provision of credit and the mobilisation of collateral are provided to the financial markets with the aim of ensuring the safety and efficiency of payments, securities and derivatives. This in turn helps to support monetary policy operations and the stability of the financial system.

To guarantee that this process continues to run smoothly, the Eurosystem has developed three action points. As there are strong business and technical synergies and inter-dependencies between the three action points, a common governance set-up for further work is required. This will be provided by the Market Infrastructure Board (MIB), the management body for the operation and development of Eurosystem market infrastructures. In addition, the Eurosystem seeks to continue its interaction with market participants with the aim of ensuring that Eurosystem services meet market needs.

“The future at your fingertips – the European market infrastructure of tomorrow” at Sibos

Monday 26 September 2016
10:15 - 11:15
Conference Room 5

Towards a new paradigm for resiliency and security

MI FORUM 2016 | GENEVA

The wholesale settlement systems of the Federal Reserve Banks are by any standard systemically important. They provide the infrastructure by which liquidity circulates through the real economy and the financial system of the United States, the means by which the Federal Reserve settles its monetary policy operations, and the platform through which the United States government issues securities to finance its operations. Given the critical importance of these systems, and the changing nature of the cyber-threats they face, traditional defences against physical attack may not be sufficient. Richard P. Dzina, Executive Vice President and Head of the Wholesale Product Office of the Federal Reserve Bank of New York, argues that systemically important financial market infrastructures may now need to consider greater diversity in a third level of resiliency and security.

The 21st century is going to be a volatile one. Around the world, societies and economies are subject to tectonic shifts with unpredictable implications for cyber-, terror, and geopolitical threats. In this unpredictable environment, one certainty remains: attacks on critical financial market infrastructure are not a matter of “if” but “when.”

This was the message I heard from General Michael Hayden, former Head of the National Security Agency (NSA) and Director of the Central Intelligence Agency (CIA), at a symposium of payments bankers in 2014. As the operator of the wholesale services for the Federal Reserve Banks, this was a sobering message on which to reflect.

The systemic importance of wholesale services

Those wholesale services consist of the Fedwire Funds Service, the Fedwire Securities Service, and the National Settlement Service. Collectively, these services constitute the "franchise" when it comes to the financial market infrastructure of the United States. That may sound like a bold assertion, but it is not an unreasonable one, reflecting at least four considerations.

First, transactional value. In 2015 we processed in excess of $1 quadrillion in Funds, Securities, and National Settlement transactions. That is a one followed by 15 zeros, and is equivalent to the gross domestic product of the United States flowing through our pipes every four days. In other words, the wholesale services represent the central conduit of liquidity – indeed, the circulatory system – of the American economy and financial system.

Secondly, inter-connectedness. In 2012 the Financial Stability Oversight Council, which is empowered under the Dodd-Frank Act to identify and monitor excessive risks to the financial system of the United States, designated eight privately owned financial market utilities as systemically important. They included the Clearing House as operator of CHIPS, a private sector Real Time Gross Settlement (RTGS) system, CLS Bank, the Depository Trust Company, the Chicago Mercantile Exchange, ICE Clear Credit, and the Options Clearing Corporation.

Although the wholesale services operated by the Reserve Banks were not formally designated as systemically important, the Board of Governors of the Federal Reserve committed to hold us to "as high or higher a standard" as it holds these private sector utilities.

This is appropriate as many of these systemically important financial market infrastructures have a critical dependence on the availability of our wholesale services in their daily operations to fund, de-fund and settle positions derived from transactions in other markets. The inverse is not necessarily true. In practice, the wholesale services operated by the Reserve Banks are the base of a pyramid on which all other systemically important infrastructures – and, indeed, the financial system of the United States as a whole - ultimately rest.

Thirdly, our role as central securities depository (CSD) and fiscal agent. As the CSD for over $70 trillion in par value of Fedwire-eligible securities, the Fedwire Securities Service functions as the central repository for the largest, deepest, and most liquid pool of collateral in the world. Moreover, in support of the fiscal agent responsibilities of the Reserve Banks, the Fedwire Securities Service facilitates the issuance, maintenance, and redemption of all Fedwire-eligible securities, performing an indispensable role in financing the operations of the United States government and those of other issuers.

Fourthly, our support for the execution of monetary policy. The wholesale services function as the platform across which the Federal Reserve ultimately settles its monetary policy operations.

Any one of these four elements would likely qualify the wholesale services as "systemic". In the aggregate they represent a staggering portfolio on which the execution of the fiscal and monetary policies of the United States absolutely depend. A wholesale service outage, or even a meaningful disruption that impairs public confidence, represents a risk to the United States with profound, and potentially unpredictable, consequences, for which the only appropriate policy response is "failure is not an option."

Flaws in the historical approach to resiliency and security

Since 9/11, consistent with industry best practice, we have sought to fulfil that resiliency mandate through dispersal of infrastructure and human capital. We have invested considerable resources to ensure operational redundancy through geographic dispersion of data centres and operating sites, real-time data replication, and split operations. These measures have yielded significant resiliency dividends, particularly against physical threats, and deserve to be heralded.

While geographic dispersion of infrastructure and human capital remains an indispensable prerequisite for responding to physical threats, and is likely sufficient for most contingency scenarios we face, it no longer suffices as the central organising paradigm for resiliency in the wake of the escalating cyber-threat. Global realities compel a paradigm shift in how we contemplate the resiliency and security of systemically important infrastructure. To borrow the vernacular of our supervisory colleagues, we must prepare for "extreme but plausible" events.

"The wholesale services operated by the Reserve Banks are the base of a pyramid on which all other systemically important infrastructures – and, indeed, the financial system of the United States as a whole - ultimately rest."

- Richard P. Dzina,
Executive Vice President and
Head of the Wholesale Product
Office of the Federal Reserve
Bank of New York

Consider, for example, a cyber-breach of perimeter security, resulting in the insertion of pernicious malware, a severe data corruption in which confidence in account balances is compromised, or even an application failure that propagates itself almost instantaneously across primary, secondary, and tertiary operating sites. An unfortunate by-product of instantaneous data replication, such a scenario risks rendering a systemic infrastructure functionally inoperable.

Aggravating the cyber-challenge, and in contrast to traditional resiliency scenarios, is the likelihood of facing an adversary that can anticipate and adapt to our contingency response in real-time. Moreover, the nature of the challenge is asymmetric. We must defend across an extended front, while the adversary need only find a single point of entry or vulnerability. These dimensions add a dynamic to resiliency planning we have not previously contemplated.

A new approach to deal with new kinds of cyber threats

In recognition of these escalating threats, the Committee on Payment and Market Infrastructures (CPMI) and the Board of the International Organization of Securities Commissions (IOSCO) recently published a consultative report providing guidance on cyber resilience for financial market infrastructures.[1]

The guidance is designed to supplement the Principles for Financial Market

Infrastructures, published by CPMI-IOSCO in April 2012.[2] It is unequivocal in its expectation that financial market infrastructures (FMIs) establish an objective of resuming critical operations within two hours of disruption, even in the case of extreme events, and regardless of whether they are cyber- or physical attacks.

For most infrastructures, this expectation remains aspirational. However, just as FMIs responded to the post-9/11 supervisory guidance to improve their resilience to physical threats by geographic dispersion of infrastructure and human capital, so will they respond to the current advice on raising their defences against cyber-attacks. There

1 The Committee on Payment and Market Infrastructures (CPMI) and the Board of the International Organization of Securities Commissions (IOSCO), *Consultative report, Guidance on cyber resilience for financial market infrastructures*, November 2015.

2 The Committee on Payment and Settlement Systems and the Technical Committee of the International Organization of Securities Commissions (IOSCO), *Principles for financial market infrastructures*, April 2012.

John Hagon

Head of Global Operations, CLS

Richard Dzina is right. The security methods adopted after 9.11, which focus on real-time data replication and geographical dispersal of people and premises, are effective against physical threats. But the same approach may not be effective against cyber-threats, such as code and data corruption.

For example, if data or code is corrupted, the corruption will likely be replicated at ancillary sites. One way to mitigate that risk is to invest in a separate operating code and database and run them at a third site alongside the existing centres. This requires investment and maintenance costs that are challenging for many institutions.

Our clients rely on the liquidity management, multi-lateral netting and settlement optimisation mechanisms provided by our system, and we cannot ask them to switch at short notice to a platform which offers only some or none of these services, or provides them in a different way.

A possible solution to this dilemma that we are considering would be to host separate versions of our data and code at a third site. The code would always be identical to the version behind the live system, and the data would be replicated at pre-defined intervals, rather than in real-time, allowing us to re-start transaction processing with data drawn from a point prior to its corruption.

One further step we have taken already to address the risk of cyber-threats is to monitor our service for signs of abnormal behaviour by clients. By mapping the current activity of our clients against their past behaviour, we can detect anomalous and potentially malicious conduct, which could be indicative of the presence of a cyber-threat, in real-time, and ensure it is addressed.

As an industry, I believe there is more that can be done. Financial systems are extremely inter-connected, but our systems will be stronger and more likely to maintain the same levels of resilience in the face of a cyber-attack if we work together, where beneficial and appropriate, rather than working in isolation.

While this poses its challenges, the industry recognises the benefits of collaboration. The sharing of ideas and reduced costs are two such examples. Ultimately, our collective goal is to strengthen the international financial system and meet the two-hour recovery time objective (RTO) recommended for financial market infrastructures by the Committee on Payments and Market Infrastructures (CPMI) and the International Organisation of Securities Commissions (IOSCO).

Two hours is an achievable objective in the wake of a physical attack. To maintain the same level of resilience in the face of a cyber-attack, we, as an industry, need to develop technological solutions to be able to identify rapidly the occurrence of a disruptive cyber-event, invoke contingency mechanisms that recover to an acceptable point in time, and resume operations within the two hour RTO.

While challenging, the industry is working towards achieving this goal. For example, a great deal of informal information sharing takes place already and greater collaborative efforts can only serve to improve cyber-security as a whole.

It is crucial to prepare and anticipate potential weaknesses in a system, and address issues as quickly as possible with minimal impact to clients. This is an area CLS is paying careful attention to – particularly in relation to detection and recovery.

Cyber-criminals are smart and becoming increasingly sophisticated. By working together to strengthen the international financial system, the threat of an attack can be reduced. The CLS model demonstrates what the industry can achieve through sound technological investment and industry co-operation.

While the investment and maintenance costs required to protect an institution against cyber-threats are challenging in the current, cost-constrained environment, it is necessary, and we cannot allow complacency to creep in.

A balance has to be struck between the mitigation of risk and expenditure on its management. The best place to strike that balance is by spending on detection and recovery, not the chimera of complete protection from cyber-attacks.

is already considerable collaboration within the industry to identify alternative solutions that can accelerate recovery from attacks, make their deployment more cost-effective, and strengthen not merely the resiliency and security of individual components, but the system as a whole.

All FMIs are making efforts to enhance perimeter security, isolate critical applications, rotate more nimbly across data centres guard against insider threats, and bolster detection and readiness. But the central question for FMIs, as they devise their cyber-security strategies, is third site capacity.

Yves Poullet

Member of the Group Management Committee and Head of Corporate Technology (CTO), Euroclear

Cyber-threats could have just as great a negative impact as the positive potential of the digital revolution. Such threats need to be treated as a strategic issue of the highest priority. Because they are systemically important, financial market infrastructures (FMIs) have a particularly heavy responsibility to maintain a degree of cyber-resilience that reduces the risk of an extreme scenario to infinitesimal proportions.

The first step in defending against cyber-threats is to invest in capabilities that reduce the likelihood of such scenarios happening. In doing so, key infrastructures face the difficulty that the 80:20 rule of management does not apply to cyber-controls. Financial market infrastructures (FMIs) need to prepare for every eventuality.

Investing in the right tools is only half the solution. Ensuring strong awareness of threats, and adherence to policy, and having staff using the tools at their disposal correctly, also minimises cyber-risk. Sophisticated cyber-defence mechanisms can easily be undermined if strong discipline is not applied in standard cyber-controls.

That is why, at Euroclear, we review our cyber-security programmes constantly, provide ongoing employee education on cyber-threats, and now stress test our cyber-security methods and procedures via covert but controlled hacking exercises (so called “Red Team Exercises”). These activities provide a constant evaluation of our standard defence mechanisms, enabling us to strengthen our defences in the face of a continuously evolving threat.

Standard defence mechanisms are used by every FMI. They include safeguarding the perimeter surrounding technology and data assets, early detection of threats, and rapid response and recovery. Such defences need strong governance to ensure measures and counter-measures adapt to constantly changing threats, and that employees, suppliers, customers and business partners maintain a high degree of awareness about the need for cyber-security.

Every market infrastructure also has extremely strong business continuity plans. At Euroclear, for example, we maintain three separate data centres, which gives us the ability to recover from many scenarios by switching production between them. Such measures are effective against physical threats such as fire, flood and terrorist attacks, but counteract a range of cyber-threats too.

However, defences based on instant replication of data can also exacerbate the consequences of a cyber-attack, by reproducing in other systems the malware or breach infecting one. For such “extreme but plausible” scenarios, this risk could be mitigated by maintaining an entirely separate data centre.

But it is not yet clear that this is the right approach. A separate system still requires the original data and the applications to make it useable, and must be fully tested on a regular basis to ensure it can support all the services required when it is activated. An alternative or complementary option to overcome a severe data corruption scenario is to have closer engagement with market participants so that data can be reconstructed from the records of the daily reconciliation process.

Guidance from the Committee on Payments and Market Infrastructures (CPMI) and the International Organisation of Securities Commissions (IOSCO) limits the time allowed to effect such data reconstruction to just two hours. Regulators and market participants expect a systemically important institution to keep maximum down-time within this very short window, and that is perfectly reasonable. The CPMI-IOSCO guidance stipulates that the deadline must be met even in extreme scenarios, but it does recognise the scale of the challenges key infrastructures might face in meeting it.

Chief among those challenges is the potential latency in detecting the cause of the cyber-incident, as in the case of an “advanced persistent threat.” With most traditional operational incidents, it is possible to pinpoint the exact time at which the issue occurred, providing certainty that data processed or applications used prior to the event are not corrupted. An advanced threat that sits inside systems for months, or even years, makes it much harder to determine what damage was inflicted, and when. Without that certainty, it is hard to be confident of the reliability of any data set or application, and so impossible to predict when a service can safely be resumed.

In those circumstances, it may be prudent to take more time to determine when the breach occurred, rather than risk resuming activity with corrupted data by rushing to meet a two-hour deadline. Designing and testing systems and processes to ensure resumption within two hours is an excellent aspiration, but it is important to take the specific circumstances of a breach into account when deciding whether it is safe to do so.

The inter-connectedness of financial markets, which increases the risk of cross-contamination, is a strong argument for putting safety first. It also points to greater collaboration between infrastructures and market participants, to exchange information about how to detect and recover from attacks. That collaboration is happening already, in both formal and informal ways, but FMIs and the authorities should be looking to intensify those efforts.

Trevor Spanner

Chief Operating Officer and Group Risk Officer, Hong Kong Exchanges and Clearing Limited

Physical boundaries are an important but not a sufficient form of defence against rapidly mutating cyber-threats. Today, actionable intelligence about upcoming cyber-attacks, and pooling of techniques to defend data and systems against them, matter a lot more than physical barriers. Intelligence of that kind requires the formal sharing of information not just with the authorities but with other financial market infrastructures (FMIs). In fact, collaboration and agreement between FMIs on cyber-security standards ensures that we do not replicate investments in a wasteful manner.

A great deal can also be gleaned from testing defences with ethical hackers, who track the evolution of threats. Informal communication with other businesses, including those outside financial services, helps too. The attack mechanisms used by cyber-criminals are rarely specific to FMIs, and trust-based collaboration can save a great deal of time and money. Trust is not easy to build, however, because businesses are understandably reluctant to share details of attacks which might expose their vulnerabilities. Nevertheless, a network of trusted relationships is a far more effective defence against cyber-threats than any amount of physical security.

We live in a connected society, so there are by definition digital bridges that will traverse any physical perimeter that surrounds an asset. Cyber-security measures have traditionally concentrated on the gateways to those bridges. However, they have to control the operator of the gateway, know who is entitled to cross the bridge, check the credentials of everybody who wants to cross it and – an issue of increasing importance - monitor their activity once they have crossed the bridge and are inside the perimeter.

There is a reason why the black market price of a social media profile is many multiples that of a credit card holder. A cyber-criminal can do much more damage with a credible social media identity than a stolen credit card. Even a cursory glance at the social media accounts of employees proves that they are more open to sharing information than security specialists would prefer. Software developers, for example, share information about the types of code they are working with, which is extremely useful to cyber-criminals looking for ways to access systems. It follows that ensuring everybody working for an organisation is mindful of the risks they create when posting material on social media is one of the investments FMIs have to make.

Clearly, the question is not whether to spend money, but how much, and in which area. Investment has to be commensurate with the risks to the organisation, but any cost-benefit analysis has also to recognise two important differences from normal return on investment calculations. The first is that the key test of a successful cyber-security investment is negative: nothing untoward happened. In this sense, purchasing security is more like insurance than investment. The second is that cyber-security investments inevitably have a shorter lifecycle than traditional investments, because cyber-threats evolve at least as fast as digital technology. Historically, we have focused our spending on preventative measures, but increasingly we are spending more on detection and response.

The framework we use for assessing cyber-threats aims to ensure any cyber-security investment is proportionate to our risk appetite. A good example of disproportionate investment is a completely separate system and site to meet an artificial deadline of restitution of service within two hours of a denial of service attack. It is simply too difficult to predict the origins and consequences of a cyber-attack to offer that guarantee. But in less unpredictable circumstances, such as loss of premises or power to fire, flood, internal sabotage or a terrorist attack, real-time replication of data means a recovery time of two hours is realistic.

Assuredly, Hong Kong Exchanges and Clearing Limited works to that expectation already. We certainly do at LME Clear, the clearing house for the London Metal Exchange, for example, where the Bank of England has specified a two hour limit on down-time. Achieving it does necessitate an alteration in procedures. When we implement real-time systems, we simultaneously change the way we process, store and grant access to data. By making those procedural changes, we also alter the mindset of the people working for us. Mindfulness – of prevention, detection and response - is definitely our best defence against a successful cyber-attack.

Historically, third site solutions rely on data replication schemes designed to restore critical functionality after primary and secondary data centres are lost. This approach looks increasingly inadequate in the face of an escalating cyber-threat. Increasingly, FMIs need to contemplate technologically diverse, off-network third site solutions that offer an impregnable firebreak, and a platform for recovery, if the core of an application suite or data set becomes corrupted.

“It may even be preferable for FMIs to develop alternative solutions, to avoid unintended concentration risk or an unhealthy measure of “groupthink”. ”

- Richard P. Dzina,
Executive Vice President and Head of the Wholesale Product Office of the Federal Reserve Bank of New York

A third level of cyber-security instead of a third site

One day perhaps we will refer to these solutions as “third level” rather than “third site,” reflecting the fact that technology is increasingly liberating us from the physical limitations of data centres, and freeing us to consider instead “metaphysical” alternatives, such as cloud or hosted solutions. However compelling the prospect, a technologically diverse third level of resiliency nevertheless raises several important questions.

Where, faced with increasing costs and diminishing returns, should an FMI draw the line on resiliency? How much insurance is enough when the odds of invoking a technologically diverse third level of resiliency may be remote, but the costs of a severe disruption from which recovery is impossible are incomprehensibly large? How can an FMI ensure the integrity of its data and software when it resumes operations after its core components are compromised? For how long should an FMI be prepared to operate in a degraded mode, and how should that assumption inform the business requirements for critical third level functionality?

FMIs will likely respond differently to these questions. They will also likely devise different technical solutions to the two hour resumption challenge set by CPMI-IOSCO, reflecting their unique circumstances and their respective assessments of the likely threats. It may even be preferable for FMIs to develop alternative solutions, to avoid unintended concentration risk or an unhealthy measure of “groupthink”. There is no need to prescribe that a common solution be applied universally across all FMIs, but

Stephen Gilderdale

Head of Customer Security Programme, SWIFT

Dispersal of sites, staff and data are measures typically deployed to ensure an infrastructure remains constantly available. Such measures help, but are not sufficient to ensure robust and comprehensive cyber-security. Provided back-up sites are logically separate, and physically secure, threats become more difficult to introduce across multiple sites. However, financial market infrastructures (FMIs) must give additional thought to cyber-security beyond traditional, availability-led thinking.

That is why best practice, and increasingly regulation, demands more. For example, tight control and authentication of access to facilities and systems (both logical and physical), thoughtful segregation of networks, encryption of data (in-flight and at rest) and measures to enforce integrity of data and software at all levels.

Whilst equipping back-up sites with an alternate technology stack is often considered a strong form of protection against targeted threats, such an approach clearly increases costs and can even degrade the risk outlook; both staff and customers must remain trained and familiar with the operation of an alternative system that is rarely used.

Of course, prioritisation of cyber-security measures remains risk-based. Financial institutions are well-practised at balancing risk versus benefit, and few today judge a wholly separate technology platform as a top priority. Nevertheless, the continually evolving threat landscape will surely drive FMIs to re-evaluate their position and look for ways of further diversifying their technology deployments.

But even the most rigorous preparations and imaginative defences cannot eliminate the risk of a breach. Equally important is the readiness of FMIs to respond fast in the event of a cyber-attack. Effective response testing must engage market participants, so that cyber-security teams can collectively practise their co-ordinated response to an attack.

Better collaboration can help. Cyber-criminals invest in attack mechanisms, and often look to increase the return on those assets by selling them to others. It follows that pooling information and intelligence between institutions will reduce the chances of multiple FMIs succumbing to the same attack vectors. In the United States, for example, information-sharing on cyber-threats between private sector firms is promoted by Executive Order.

However, collaboration can take many forms, and fragmentation makes effective cyber-intelligence management more complicated. Details of threats are disseminated by automated systems as well as by commercial forensics firms. In addition to national and regional Computer Emergency Response Teams (CERTs) and industry-based Information Sharing and Analysis Centres (ISACs), a great deal of informal collaboration takes place between security officials at individual firms. Furthermore, concerns about the distribution and use of information can deter some organisations from submitting valuable data in the first place.

FMIs are well placed to help. Market infrastructures are natural entities with whom participants can share intelligence; they can help create shared solutions and, as a consequence, minimise the associated cost of defence for the industry. Market participants look to FMIs for highly available and resilient shared services – strong cyber-security is key, and perhaps they should also look to FMIs to play a larger role here too.

there is an onus on all FMIs to reflect on how best to respond to an issue of fundamental importance.

The new CPMI-IOSCO cyber-guidance also exhorts FMIs to develop contingency plans for events in which they fail to resume operations within two hours. Both in the Wholesale Product Office and across the Federal Reserve System we are considering remedial actions to mitigate customer and market impacts in the event of a wholesale service disruption from which we cannot recover on a same day basis.

This work proceeds on multiple fronts, including analysing and parsing our transaction flow to identify systemically important activity, and exploring alternative routes to process that activity via other channels and service providers. Later this year, we will be conducting table-top exercises with systemically important customers and FMIs to test our hypotheses and procedures.

But we are not deluding ourselves. No matter how mature our framework for responding to protracted outage scenarios, no matter how sound our procedures, and no matter how tested our protocols, we would never want to rely on such measures. Our real objective is to invest in resiliency and security measures that ensure that we never find ourselves in such a position.

The elements of a new resiliency and security paradigm

What would such a set of measures actually look like? As a former Army officer, I counsel against constructing a Maginot line so inflexible that its rigidities are easily subverted by a creative and nimble adversary. We should aim instead to develop a coherent and integrated system that relies upon all of the classical elements of defence, but depends on none of them exclusively.

We need perimeter security to keep the adversary outside of the environment; defence in depth to safeguard our most critical assets; sophisticated intelligence to understand the tactics of our adversaries; robust surveillance to monitor for intrusion and ensure the integrity of the environment; rapid response to fend off attacks; effective collaboration with allies to enhance collective security; and a strategic reserve to respond deftly in the event of loss.

Combinations of measures of this kind do more than enhance security and resilience. They also provide an extremely effective deterrent by raising the costs our adversaries must bear to perpetrate a successful cyber-attack. In protecting the wholesale services of the Federal Reserve Banks, we aspire not merely to a commercial standard of resiliency, or even to a supervisory standard, but to something approaching national security grade. In this sphere, either intentionally we are progressing or inevitably we are regressing: there is no idleness.

"Cyber-resilience in a changing world" at Sibos

Monday 26 September 2016
09:00 - 10:00
Conference Room 2

The quiet revolution that is transforming post-trade securities services in Europe

MI FORUM 2016 | GENEVA

The European financial market infrastructures of 2021 will look like radically different from their predecessors of today. But what is driving that transformation is not the widely anticipated wave of mergers and acquisitions of central securities depositories (CSDs). Instead, say Nadine Limbourg, Senior Market Manager, Market Infrastructures at SWIFT, and Isabelle Olivier, Head of Securities Initiatives and Payment Market Infrastructures at SWIFT, the securities market infrastructure of Europe is being re-built spontaneously by CSDs and custodians in pursuit of practical solutions to the new challenges created by regulations and transformative projects such as T2S.

There is grandstanding in business as well as politics. CEOs like to make grand strategic gestures. Investment bankers work hard to find the businesses to merge or sell or buy that enable them to do so. Journalists, eager to inject personality and drama into the intrinsically dull routines of corporate money-making, populate the business pages with deals and rumours of deals.

In reality, industries are transformed not by great events but by hard work, which occurs unseen. This is certainly true of the central securities depositories (CSDs) that serve the European securities industry. A long-anticipated wave of mergers and acquisitions between CSDs has failed so far to materialise, but an operational revolution is nevertheless in train.

Regulation is the driver of change

What has sparked this revolution is the conjunction of several regulatory and harmonisation initiatives. Some have had a direct impact on CSDs. TARGET2-Securities (T2S), the pan-eurozone settlement platform, and the accompanying Central Securities Depositary Regulation (CSDR) are gradually harmonising and centralising the settlement activities and revenues of the CSDs.

The CSDR has already shifted European markets on to a common settlement timetable of trade date plus two days (T+2) as part of the preparations for the transition to T2S. The T2S project is now migrating the majority of euro-zone countries - and some non-euro markets, in the shape of Denmark, Hungary, Romania and Switzerland – on to a single settlement platform.

Importantly, the CSDR also invites CSDs to choose what services they will offer, and where.

Other regulations have also created new opportunities for CSDs. The Alternative Investment Fund Managers Directive (AIFMD), the European Market Infrastructure Regulation (EMIR) and the upcoming revisions to the 2007 Markets in Financial Instruments Directive (MiFID II) are creating a new line of work for infrastructures and custodians: regulatory report services and storage.

CSDs are positioning themselves to defeat the threats and exploit the opportunities created by T2S and other regulatory initiatives. Yet they must also maintain their existing settlement, custody, issuance, asset servicing and - in some cases – banking services. This has created a tension between business-as-usual, mandatory adaptations to regulations, and long-term strategic decision-making.

After all, every CSD must continue to service existing accounts. Almost all CSDs in the eurozone are transitioning to T2S, necessitating technical decisions over integration technologies and connectivity. Even CSDs outside the euro-zone and T2S are bound by CSDR. Its penalisation of late settlement, and insistence that CSDs allow users to choose account structures, also need implementation.

To impose late settlement penalties, CSDs have to devise and build systems to collect buy-in data from users, source market prices to calculate and charge the correct amount, and isolate and communicate exemptions. Since T2S insists on omnibus accounts, while CSDR demands that clients be offered segregated as well as omnibus accounts, CSD systems must offer both.

CSDs need to make choices

But there are strategic, as well as technological, choices to be made. T2S truncates the core settlement revenues of CSDs, so a change of business model is involuntary. CSDR recognises this. Its CSD licensing system effectively invites CSDs to decide if they wish to offer services in other member-states of the EU, seek the business of non-domestic issuers, or acquire a banking licence.

The ability to settle in central or commercial bank money, offer services or open branches in third countries, and solicit foreign issuer business, is rich in opportunities for European CSDs. Any CSD prepared to seize them has the chance to turn itself into a pan-European, regional or sub-regional investor or issuer CSD - or both - in, say, the Nordic or central and eastern European markets.

The choices of CSDs will be conditioned by multiple factors. Chief among them is the confidence of the management in their ability to shift from a domestic to a broader canvas. They will also have to upgrade systems and procedures to adapt to the price and fee disclosure, additional capital, liquidity monitoring, governance and recovery and resolution requirements set by the regulators.

The competitive environment will also influence the strategies of CSDs. After all, their most valuable clients (the sub-custodians) and the clients of their most valuable clients (the global custodians and global investment banks) are also assessing their strategic options, not just in terms of extending their services into new markets and asset classes, but in terms of mergers and acquisitions.

CSDs and custodians experiment in collateral management services

Some global custodians have considered investing in CSDs of their own, though these initiatives are now on hold. Initially, their interest was sparked mainly by the requirement under EMIR for central counterparty clearing houses (CCPs), whose importance as a source of demand for collateral was being greatly expanded by the mandatory clearing of OTC derivatives, to hold collateral posted by clearing brokers at a CSD.

Anticipation of an EMIR-driven increase in demand for CCP-eligible collateral was also a major factor behind the tri-party collateral management alliances formed between leading sub-custodian networks in Europe (such as BNP Paribas and Citi) and the international CSDs (Clearstream and Euroclear). They enable broker-dealers to access as collateral assets held in domestic markets.

The lack of links to transfer collateral across borders is a longstanding criticism of the market infrastructure of Europe. Even the Correspondent Central Bank Model (CCBM), introduced at the advent of the euro to help central banks advance credit against collateral held elsewhere, was long undermined by a requirement to transfer assets to the CSD into which they were first issued.

This chronic difficulty in moving assets between domestic markets forces payments and custodian banks to maintain collateral "buffers" in domestic CSDs to access credit from national central banks. T2S promises to solve this problem by allowing banks and tri-party agents to settle collateral trades on its 20-market settlement platform, effectively creating a single European pool of collateral.[1]

1 See Marc Bayle, "The future of collateral management in Europe and beyond," MI Forum magazine, issue 2, 2014, pages 142-7.

Co-operation more common than competition or consolidation

Partnerships of this kind between banks and infrastructures indicate co-operation is as probable a response to the threats and opportunities created by regulation as competition or consolidation. In fact, Clearstream has formed partnerships with BNP Paribas, BBVA, Citi, Erste Bank and Intesa San Paolo, in which it will settle trades, and the sub-custodians service the assets.

A similar arrangement is in place between Northern Trust (as global custodian), Euroclear France (as the CSD able to settle trades in T2S) and Deutsche Bank (as account operator and asset servicing agent in domestic markets). In both the Clearstream and Northern Trust cases, the specialists – CSD, sub-custodian and global custodian – have decided not to stray beyond their core capabilities.

The chief rationale for these partnerships is that they combine efficiency (a reduced need for local liquidity) with service (proximity to the local market), but it is highly significant that they also allow specialists to play to their strengths. This is a somewhat unanticipated outcome of T2S, which was originally expected to reduce the reliance of global custodians and investment banks on CSDs and sub-custodians.

The rise of the specialist service provider

The hierarchical settlement and custody model of the past (global custodian, sub-custodian, CSD) is giving way to a new division of labour. It is one in which banks and CSDs combine best-of-breed skills to deliver to buy- and sell-side clients bespoke blends of settlement, collateral management and liquidity management, and asset servicing. Even specialist providers of compliance or regulatory reporting are no longer unthinkable.

To realise this prospect, however, specialist providers must be able to inter-operate efficiently. If the transactions costs of inter-operability are too high, the vertical integration of specialist skills will become unavoidable. New technologies (such as distributed ledgers) may eventually play some part in reducing transactions costs, but the real key to efficient networks is standardisation.

The importance of standards

Here, there are potential obstacles. A first example is that both CSDR and EMIR favour Legal Entity Identifiers (LEIs) over Business Identifier Codes (BICs) as the best way to identify counterparties, but CSD and custodian bank systems have yet to complete a conversion from BICs to LEIs. Similarly, although T2S uses ISO 20022 messages, the European securities industry still uses ISO 15022 or even proprietary messages to exchange information.

Custodian banks can insulate their clients from non-compliance with these standards for a time, but not forever. If CSDs and custodians are to exchange the richer information required by CSDR, let alone to grow their businesses, adoption of a common version of ISO 20022 messages is essential. This is one reason why SWIFT is encouraging CSDs to sign the ISO 20022 harmonisation charter.[2]

2 See Andrew White, "Everybody benefits from standardising the ISO 20022 standard," MI Forum magazine, Issue 3, 2015, pages 104-115.

These changes will take time to implement, and their outcome is hard to predict. It is not yet clear whether the manoeuvres and adaptations now taking place represent the beginning, the middle or the end of the transformation of the securities markets of Europe. Work needs to be done to complete the current process, let alone address challenges that have yet to disclose themselves.

But it is already obvious that the moves initiated by regulations and harmonisation measures such as T2S are transforming the post-trade architecture of the European securities industry more profoundly than the regulations themselves. That is because they are between them delivering an infrastructure off which new and existing businesses can provide genuinely innovative services.

"EU securities markets transformation - is the glass half empty or half full?" at Sibos

Monday 26 September 2016
09.00 – 10.00
Workshop A

The CMU promises a joined-up approach to integrating EU capital markets

MI FORUM 2016 | GENEVA

The Capital Markets Union (CMU) is the latest effort by the European Commission to fulfil its longstanding ambition of creating a single capital market capable of financing growth across the European Union, attracting investment from outside, and – importantly – redressing the structural imbalances within the post-crisis euro-zone. It is an ambitious and widely welcomed plan, for a single European capital market has proved remarkably elusive. The willingness of the authors of the CMU to re-visit previous work as well as add to it is a positive sign, says Natasha de Terán, Head of Corporate Affairs at SWIFT.

A stated ambition of the Treaty of Rome of 1957 was the free movement of capital in Europe, but its realisation was long obstructed by exchange controls. These did not disappear until the 1990s. Technical, legal, regulatory and fiscal barriers have never completely disappeared, in spite of repeated efforts to clear them. Indeed, the Single European Act of 1986 was designed to leapfrog the barriers, by substituting mutual recognition of national regulatory regimes for the unattainable goal of harmonising them.

The Cecchini Report[1], published by the European Commission in 1988, proposed a bonfire of obstructions that was forecast to add 1.5 per cent to European Gross Domestic Product (GDP) once it was complete. But mutual recognition proved an ineffective tool in eliminating barriers. After another decade of disappointing progress, and with the single European currency just a year away, in 1998 the Commission adopted a Financial Services Action Plan. Its 42 measures were designed to accelerate the integration of European markets into a single pool of capital comparable with the United States.

A capital market fit to compete with the US remains remote

More than a decade and a half later, the Commission confessed in the opening paragraphs of the Action Plan on Building a Capital Markets Union - the document by which it launched the CMU on 30 September 2015 - that “Europe’s capital markets are still relatively underdeveloped and fragmented.

1 Paolo Cecchini, *The European Challenge 1992: The Benefits of a Single Market*, Commission of the European Communities, 1988.

The European economy is as big as the American one, but Europe's equity markets are less than half the size, its debt markets less than a third. The gap between member-states is even bigger than that between Europe and the United States."[2]

The CMU aims to address the most conspicuous of the differences between the European and the American capital markets: the continuing reliance of European business on bank, rather than equity or bond, financing. The fostering of a large and liquid securitised debt market is chief among the ambitions of the framers of the CMU, though it also launched consultations on how best to promote the growth of venture capital and covered bond markets.

Regulatory obstacles up for review

A second striking feature of the CMU at its launch was a "call for evidence" on the cumulative impact of financial regulation. This last objective marked a recognition that the quantity of regulation imposed on the European financial markets since the acute phase of the financial crisis in 2007-08 might well have created burdens, inconsistencies, contradictions and unintended consequences that are suppressing rather than enhancing the further integration of the capital markets of Europe.

The invitation to contribute to the consultation also recognised that in some areas, regulation had made insufficient progress. The failure to clear the 15 specific barriers to cross-border securities clearing and settlement identified in the two Giovannini reports of 2001[3] and 2003[4] is an obvious case in point, made urgent by the current transition to TARGET2-Securities (T2S), the pan-European securities settlement system.[5]

But equally intractable barriers exist beyond market infrastructure. They include differences in national laws on securities issuance, the enforceability of collateral contracts, the ownership of property, and insolvency. Even apparently minor differences between fiscal, legal and regulatory rules create enough uncertainty to undermine the movement of capital across national borders.

In theory, EU institutional reforms such as T2S, and regulations and directives such as the Prospectus Directive, the Transparency Directive, the Market Abuse Regulation (MAR), the European Market Infrastructure Regulation (EMIR), the Benchmark Regulation, the proposed Credit Ratings Agencies Regulation (CRA), the Central Securities Depositories Regulation (CSDR) and the Markets in Financial Instruments Directives of 2007 (MiFID I) and 2017-18 (MiFID II), have and will between them remove barriers to the cross-border issuance, trading, clearing and settlement of securities.

Certain of these changes have already precipitated a restructuring of the post-trade infrastructure of the European securities industry, and have the potential to help integrate European capital markets. "CMU is a very high level policy initiative, yet huge amounts of harmonisation have already been achieved through CSDR, EMIR and T2S," points out Alan Cameron,

2 European Commission, *Action Plan on Building a Capital Markets Union*, 30 September 2015.

3 The Giovannini Group, *Cross-Border Clearing and Settlement Arrangements in the European Union*, November 2001.

4 The Giovannini Group, *Second Report on EU Clearing and Settlement Arrangements*, April 2003.

5 See Alberto Giovannini, "T2S will reverberate through the European capital markets," MI Forum magazine, issue 2, 2014, pages 76-80.

“The CMU project is giving extra impetus to the EMIR review, encouraging European policymakers to look at rules and regulations such as EMIR holistically.”

- James Cunningham,
Senior Adviser for Public Policy and Regulatory Affairs at BNY Mellon.

Head of Relationship Management at BNP Paribas Securities Services. “These all pre-date CMU.” So far, so good, counter proponents of CMU. Where CMU will make a difference, they argue, is in reversing the law of unintended consequences.

EMIR and CSDR prove unhelpful to integration

EMIR, for example, fulfils a Group of 20 (G20) obligation on derivatives market participants to report details of both exchange-traded and OTC transactions to a trade repository. But by permitting multiple trade repositories to compete for business, and by obliging both parties to a transaction to report it, the regulation has created problems of matching and reconciliation between the operators of the six repositories. The result is duplication, and fresh forms of fragmentation, without yet delivering in full the advertised benefits for the management of systemic risk.

So it is encouraging that CMU will likely accelerate a re-consideration of EMIR reporting obligations. “CMU is both a set of EU aspirations of what European capital markets should look like in 2019, and a set of specific initiatives,” explains James Cunningham, Senior Adviser for Public Policy and Regulatory Affairs at BNY Mellon. “EMIR certainly falls within its scope. EMIR would have been reviewed in any event, but the CMU project is giving extra impetus to the EMIR review, encouraging European policymakers to look at rules and regulations such as EMIR holistically, and to focus on identifying unintended consequences. It is hoped that the increased focus that CMU will bring to this issue will lead to proposals from the EU authorities.”

The implementation of EMIR has also struggled to keep abreast of the global reality of trading and clearing in derivatives, by insisting the European Securities and Markets Authority (ESMA) decide whether non-EU central counterparty clearing houses (CCPs) were regulated to a sufficiently high standard to be used by European counterparties. While it is reasonable for EU regulators to check the credentials of non-EU CCPs, the apparently extra-territorial extension of the regulation created some tensions with market participants.

Similar challenges had to be overcome in the implementation of CSDR, which subjects non-EU CSDs to authorisation by ESMA. Naturally, market participants were concerned this might obstruct the flow of securities transactions between EU markets and Asia, Switzerland and the United States. Likewise, the imposition by CSDR of fines for late settlement has prompted warnings of a negative impact on liquidity in the European bond and repo markets. A properly functioning CMU, one of whose stated aims is greater liquidity, will make it easier to solve problems of this kind.

More progress needed on securities law

If EMIR and CSDR contained elements that were open to the charge of impeding rather than advancing progress towards a single European capital market, there are other fields in which more rather than less needs to be done. The most obvious barrier, apparent since at least the Giovannini Reports of 2001-03, is legal uncertainty over how securities can be held, cleared and settled across borders. Repeated initiatives aimed directly at this issue – the Settlement Finality Directive (SFD), the Financial Collateral Directive (FCD) and the Shareholders’

“The most obvious barrier, apparent since at least the Giovannini Reports of 2001-03, is legal uncertainty over how securities can be held, cleared and settled across borders.”

- Natasha de Terán,
Head of Corporate Affairs at SWIFT

Rights Directive (SRD) - have failed to resolve it. A proposed Securities Law Directive failed altogether.

In March 2016, the Commission established the European Post Trade Forum (EPTF) to help drive the CMU to a more successful outcome. "Most of the private sector barriers identified in the 2001 Giovannini Group report have been removed as a result of CSDR, T2S and EMIR," says Paul Symons, Head of Government Relations at Euroclear. "But public sector issues like conflicts of law and divergences in securities ownership law and structures remain. The EPTF working group is in its early stages and is looking at the current state of the post-trade industry, and then it will identify issues that could be addressed through CMU."

The divergence of national insolvency laws is likely to be an early target. The mission to solve the longstanding problem of what happens to securities belonging to third parties in an insolvency – especially those posted as collateral – was given additional impetus by the Alternative Investment Fund Managers Directive (AIFMD), which came into force in July 2014, and the fifth iteration of the Undertakings for Collective Investment in Transferable Securities Directive (UCITS V), which came into effect in March 2016.

This was because AIFMD and UCITS V increase custodian banks' liability for making investors whole if their assets are lost, including in insolvencies. "Harmonising the rules on insolvency and securities ownership is a really important issue for CMU," says James Cunningham of BNY Mellon. "Both because safety in the custody chain is a fundamental building block of a CMU, and because the approach taken by UCITS V and AIFMD, especially in relation to asset segregation, is flawed and incapable of generalisation to all types of investors."

As the CMU Action Plan acknowledged, it is obvious that a single EU capital market cannot develop as long as the ownership of securities cannot be determined with legal certainty when the issuer and the investor are located in different member-states, or when securities belonging to investors in one member-state are held on their behalf by custodian banks in a different member-state. That uncertainty is an obstacle to cross-border trading and investment in general, and collateralisation and securitisation in particular. In the EU, progress in securities law continues to lag behind the development of securities market infrastructure.

"Single market and Capital Markets Union - the future role of Financial Markets Infrastructures" at Sibos

Monday 26 September 2016
15.30-16.30
Conference Room 3

Linking interbank payment systems across borders and currencies: how easy is it?

MI FORUM 2016 | GENEVA

The dream of making cross-currency payments faster, cheaper and more transparent by building simple links between domestic payment systems has proved elusive, but refuses to die. It can be done, says Harry Newman, Head of Banking at SWIFT. But he warns that success is rare and the obstacles to success are great, so that correspondent banking remains the preferred – though far from perfect – alternative.

Superficially, linking the payment market infrastructures (PMIs) of different countries ought to be easy. After all, PMIs are restricted to a single asset class (cash) and exchange nothing but digital information (mainly instructions to move cash from one account to another). Surely we should be able to build a technical link and exchange messages? Well, the realities are harder to adjust than a superficial assessment suggests.

Links do not lower currency barriers

Chief among them is the fact that different countries generally use different currencies. In any currency pair, there is not one asset to be exchanged but two. To transfer cash from, say, a Sterling account to a US dollar account entails a foreign exchange transaction. Since PMIs do not normally exchange currencies, this necessitates the involvement of at least one bank to execute the trade.

More often, and especially in minor currencies, the foreign exchange trade also requires not one bank, but two. This is because cash is an asset, issued into the financial system by a central bank or government ministry. Given the importance of monetary policy to sovereignty, price stability and economic growth, central banks are reluctant to issue liquidity in their currency to any bank they do not regulate.

An entirely valid solution to foreign exchange for PMIs would be to appoint a single bank (or even multiple banks) as foreign exchange agent(s). The PMI could then provide a foreign exchange trade execution service as an integral part of the link. However, foreign exchange trading is a business for which banks compete fiercely, and it is unlikely that other banks would make use of a link that gave currency business to a competitor. This solution to the issue makes it unattractive to others.

Another option would be to issue instructions in the currency of the receiving country only. However, this merely shifts the foreign exchange issue elsewhere. To be exact, the sender has to maintain an account with an agent in the receiving country in the relevant currency, like a nostro account.

Any such link between two jurisdictions is also likely to require oversight by regulators in both countries, as both PMIs will be processing transactions in a currency which is not their own. Central banks will need to reach agreements to do that. This makes regulation more awkward

than current arrangements, in which the sending bank connects with one payments system and the receiving bank with the other, and each bank is regulated separately in its own jurisdiction.

Regulatory, scheme and data privacy barriers abound

But the barriers are not restricted to the regulatory (regulation in both countries), the infrastructural (access to the settlement system), or the commercial (competition for foreign exchange business). Each jurisdiction has different laws, regulations and reporting requirements. Each also has specific "schemes"[1] defining payment types, as well as different technical standards, such as identifiers and message formats. Market practices are attuned to local markets. No country will change these simply to facilitate cross-border payments.

Even between jurisdictions that use the same currency, these formal and informal barriers have proved difficult to dislodge. In the Single Euro Payments Area (SEPA), where 19 of the 34 countries share a currency, years of effort to harmonise payments reporting, business and operational rules, and market practices, have still not spared payments banks from having to adapt to multiple national regulatory regimes.

Differences in business rules and practices translate into variations in message standards, even if they are both using a global standard such as ISO 20022. It is possible to overcome these - and there are examples of how it can be done, such as the approach pioneered by the International Payments Framework Association (IPFA) - but it always requires work. Overcoming barriers is more than a mapping issue.

Data privacy is another barrier to linking payment systems across borders. Inside individual countries, local banks apply national data privacy laws on a day-to-day basis. Any link carrying payments between any two countries, on the other hand, is subject to the data privacy laws of both jurisdictions. Banks active in multiple countries are used to dealing with different local data privacy requirements, but few local PMIs are currently equipped to take on the load of managing multiple data privacy requirements.

Technical barriers also a problem

The barriers are technical as well as regulatory. National "schemes," which set the technical standards for moving money, vary between systems in the same country, let alone across borders.

Different systems are implemented in ways that create technical and operational barriers which have to be bridged. Security is always an issue too, as different countries have different security arrangements to comply with national rules, such as the list of "schemes" that are permitted. The challenge is not insuperable, because it is a matter of investing in suitable technical infrastructure, but it is still non-trivial.

Using the same vendor for two payment systems could make some of the technical challenges easier to overcome, but that still leaves non-technical issues unaddressed. Once all the mappings, technical variations, different market practices and regulations are resolved, a bank or near-bank is still required to complete the foreign exchange transactions and be responsible for making payments in the relevant payment system.

1 "Scheme" is payments industry shorthand for a collection of business rules and technical standards for the execution of payment transactions within a particular community.

ACH links likely to founder on settlement, not standards

There are two principal challenges to cross-border links between domestic payment systems such as ACHs, and the hardest to clear is not message standards but settlement mechanisms, says Jeremy Light, Managing Director, Accenture Payment Services.

Domestic payment systems process high volumes of local payments quickly and efficiently, but they tend not to be inter-operable with payments systems in other countries. A bank in France, for example, can send a payment with ease to a beneficiary of another bank in France through the local automated clearing house (ACH).

But the same bank cannot use the domestic ACH to send a payment directly to a beneficiary in Australia. Instead, it needs to use its correspondent banking network - a route that is typically slower, more expensive and more error-prone. So how can ACHs be linked so that they are inter-operable, enabling seamless, fast and efficient payments across borders?

To make this possible, several factors need to be addressed. They include governance, liability agreements, financial crime controls and foreign exchange mechanisms, but the two most important factors to get right are messaging and settlement. Common messaging standards permit inter-operable processing, while cross-border settlement necessitates a mechanism that allows unrelated banks in different countries to settle payments with each other.

On the messaging side, the obvious answer is to use the ISO 20022 standard. ISO 20022 is being widely adopted by banks and ACHs around the world, and not just for payments either, but for other financial services as well. However, ISO 20022 is a flexible framework, not a rigid message set, which can create incompatibilities which hamper inter-operability.

ISO 20022 has a data dictionary for common data format definitions, for example. But the actual data elements used by an application are dependent on the needs of the application, and different applications can have different needs. Use of ISO 20022 does not therefore guarantee inter-operability between payment systems that use it.

There is an analogy with domestic debit card "schemes"[1]. They use the older ISO 8583 standard, but that does not make them compatible with international card schemes such as Visa, MasterCard and American Express, even though the international "schemes" also use ISO 8583. This is why domestic debit cards often cannot be used outside their home country, or on-line.

Where the international "schemes" are also ahead of domestic alternatives is in the other important factor in cross-border inter-operability between ACHs: efficient settlement. A core element of the international card value proposition is the provision of inter-operable payments around the world. A Visa card issued by a bank in Germany, for example, can be used to purchase goods from a merchant in Singapore.

The mechanism works because Visa enables the bank that issued the card in Germany to settle with the bank used by the merchant in Singapore. This is a major competitive advantage of the international card "schemes" in cross-border payments, but it took them years to develop the settlement networks on which the service depends. It will be hard for ACHs to match them quickly.

A settlement mechanism that enables payments between banks across borders is the larger of the two obstacles to inter-operability between ACHs. This is not surprising. Settlement is a challenge to cross-border inter-operability between any pair of domestic payment systems. Exchanging messages to a common standard, such as ISO 20022, is important and achievable. It is adding the settlement component that ACHs will find most difficult to accomplish.

1 "Scheme" is payments industry shorthand for a collection of business rules and technical standards for the execution of payment transactions within a particular community.

In sum, the list of obstacles to direct links between payment systems in different countries is a long one. It includes the need for access to national settlement systems, dual regulation, meeting security concerns, differences between laws, regulations, business rules, market practices and reporting requirements, variations in message standards, misgivings about data privacy, and technical and technological mismatches.

How would interlinking PMIs work to execute cross-border transactions?

However, it is safe to assume that these obstacles can be overcome. Once they are, each PMI can carry payment types defined in other PMIs, exception handling between the two systems can be defined, and different national addressing schemes can be taken into account.

Even regulatory barriers can be cleared, though the number of regulators increases in line with the number of PMIs involved in the transaction.

At that point, the most difficult issue that remains is foreign exchange. Imagine that a firm in the United Kingdom needs to pay a US dollar account holder in the United States. There are three ways in which the payment can be made. The first is for the payment to be made in US dollars. The second is for the payment to be made in Sterling. The third is for the payment to be made in Sterling and converted to US dollars before it lands in the account.

To send a payment in US dollars, one of three things must be true. Either the sending bank has an account in the US dollar payments system (in which case it is a bank regulated in the United States), or it can clear and settle directly in the United Kingdom payment system because the Bank of England is entitled to settle US dollar transactions, or it is using a correspondent bank to access the US dollar payments system.

If the payment is sent in Sterling, the reverse applies. Either the receiving bank has a settlement account in the United Kingdom settlement system (in which case it is a bank regulated in the United Kingdom), or it maintains a Sterling account in the United States payments system (because the Federal Reserve is entitled to settle Sterling transactions), or it is using a correspondent bank to access the Sterling payments system.

The idea of central banks offering banks remote access to their settlement systems through reciprocal currency accounts can scarcely be described as a revolutionary or even particularly compelling notion. A small class of regulated institutions already belong to several central bank-operated payment systems. Links that work in that fashion add nothing new.

The third option, of sending the payment in Sterling and converting it to US dollars, offers nothing different either. Unless the foreign exchange bargain is executed by the PMIs or by some separate mechanism within the proposed link – neither of which is likely – each system would have to appoint one or more correspondent banks in the other country to execute its foreign exchange business.

In short, correspondent banks continue to play a crucial role. Even in the examples of inter-linked PMIs that do exist - such as those between PMIs that subscribe to the standardised operating framework devised by IPFA - there always remains a correspondent bank supporting each system to execute foreign exchange transactions and take responsibility for payment.

Could central banks provide a solution?

A direct link operated by central banks could reduce this reliance on correspondent banks. If the central banks operating the link open settlement accounts for banks in their respective currencies, or execute foreign exchange trades on behalf of banks using their settlement systems, there would be no need for correspondent banks.

However, outside a fixed exchange rate regime, it is hard to see why central banks would assume such a risk-taking role in the foreign exchange markets.

That said, there are cases of central banks offering foreign currency settlement. When the euro was introduced, the European Central Bank (ECB) linked the domestic payment systems of member-states. Until it became obvious they would remain outside the euro, non-euro central banks were allowed to settle euro transactions (though not to generate liquidity).

Other central banks host foreign currency clearings, usually in major currencies such as the US dollar and euro, with the aim of allowing banks to make foreign currency transactions in the local time-zone. In this case, they are typically not offering final settlement: correspondent banks usually continue to settle the amounts net at the end of the business day through TARGET2 (for euro) and Fedwire (for US dollars).

This is unsurprising. Even if it provided useful support to settlement links between payment systems, central banks are cautious about encouraging offshore uses of their currency, since it impinges on their control of domestic monetary conditions.

The understandable reluctance of central banks to endorse offshore settlement, or engage in foreign exchange on behalf of commercial banks, places limits on the effectiveness of links between payment systems. It means that the viable solutions for inter-linking of payment systems will continue to involve a bank (or near-bank) to execute foreign currency transactions and assume final responsibility for settling the payment.

It follows that correspondent banks - one in each country holding an account with the other, and taking responsibility for the foreign exchange and the payment - will remain by default the principal linkages across borders. They have the merit of operating in an open and competitive market that offers users choice. The correspondent banking model also works, and it can facilitate payments between any pair of currencies.

That said, correspondent banks are seen as a slow, opaque and relatively expensive method of moving cash between currencies. Even as they respond to pressure to improve both quality and transparency, they remain vulnerable to new entrants which hold accounts directly at payment systems in multiple countries. So the ultimate question is whether correspondent banking can evolve sufficiently fast to provide a better service and payments experience capable of competing with the new entrants. But that is a story for another time.

"Payments inter-operability across communities and currencies" at Sibos

Tuesday 27 September 2016
10.15-11.15
Conference Room 2

How FMIs are improving operational efficiency in the Asian fund industry

Asian fund markets are growing, and flows between them are bound to increase as a trio of regional fund passport schemes come into effect, but variations in communication standards and levels of automation between markets will obstruct progress unless they are addressed. The recently formed Asia Funds Standardisation Forum (AFSF) is doing exactly that. Alexandre Kech, Head of Securities Markets and Standards for SWIFT in Asia Pacific, discussed how financial market infrastructures (FMIs) are driving operational risks and costs out of the Asian funds industry with Isaac Wong, Director, Product Management, Investment Funds, Euroclear; Supranato Prajogo, Director of KSEI, the Indonesian central securities depository; Joong Hoon Park, Head of Fund Planning at the KSD, the Korean central securities depository; Kitti Sutthiatthasil, Head of Strategy at the Stock Exchange of Thailand; and Boon-Hiong Chan, Director and Head of Market Advocacy, Asia Pacific, at Deutsche Bank.

Kech: What is the state of domestic fund automation in Asia as a whole and your market in particular, and how important is the ISO 20022 standard to your efforts to increase the level of automation?

Sutthiatthasil: Thailand is seeing a lot of improvement in terms of the level of automation. Although there is as yet no standard agreed for communicating orders, the exchange is working with market participants, the regulator and the distributors on standardising mutual fund order processing. We expect to launch our new fund platform next year. At present, the agreed standards are local, but we are considering adoption of international standards for funds distributed across borders.

Park: We already use international standards for cross-border trades. Korea Securities Depository (KSD) has operated a domestic fund platform called FundNet since 2004, when it was created in co-operation with the asset management industry and the government. FundNet automates the whole process, from subscription, redemption or switch, through trade matching and delivery instructions, to settlement and delivery. But in the domestic market FundNet uses proprietary local standards tailored to Korean participants only. However, the Offshore fund Service Platform (OSP), which KSD has offered since 2012 to asset managers and fund distributors selling to domestic investors in Korea, does use the ISO 20022 standard. By converting domestic proprietary standards into ISO 20022, and vice versa, OSP facilitates communication with transfer agents and other fund service providers based offshore.

Prajogo: Indonesia has explored the automation of domestic fund processing by establishing a fund platform called S-Invest. It drew on the experience of our colleagues at the Korean central securities depository (CSD) and on local market participants, to make functional adjustments specific to the Indonesian market. The system was launched in August this year. The new system will provide an integrated solution for automating the whole process of order routing - subscription, redemption and switching - as well as automating post-trade exchanges between fund managers, custodian banks, fund distributors and brokers in electronic formats. In terms of message standards, ISO 20022 is not used at this point, mainly because S-Invest initially supports domestic funds only. ISO 20022 is likely to be used once offshore investment services are introduced.

Chan: Asset managers and fund distributors in Asia face varying levels of automation. As we have just heard, there is an established market utility in Korea, and we will soon have something similar in Indonesia and Thailand. These utilities promote high levels of automation. But in many other markets in Asia, the level of manual processing remains a challenge. So Asian markets are mixed in terms of automation, although trending in the right direction. On the adoption of standards, we see two types of clients. The banks that are servicing global custodians adopt ISO standards to ease their connectivity to offshore fund and client groups, while the local and regional players are not yet under intense competitive pressure to adopt them, although ISO formats such as 20022 will be adopted gradually by local and regional banks. The Asia Fund Standardisation Forum (AFSF) is helping the industry to attain a higher level of standardisation.

"There is an established market utility in Korea, and we will soon have something similar in Indonesia and Thailand. These utilities promote high levels of automation. But in many other markets in Asia, the level of manual processing remains a challenge."

- Boon-Hiong Chan, Director and Head of Market Advocacy, Asia Pacific, Deutsche Bank

Kech: Does the limited take-up of international standards reflect the language barrier and, if so, are the global custodians happy to use domestic standards as well, or are they pressing for international standards instead?

Sutthiatthasil: In Thailand, language is not the barrier. Most of the communication is actually done in English. The problem is that local market participants cannot see a real need to adopt international standards for a domestic process. Of course the leading houses all use international standards. As a Thai clearing house, we ourselves accept SWIFT message formats from international players, but use the local version of SWIFT when connecting to domestic players.

Park: In Korea, the low use of the ISO 20022 standard reflects history. When we developed FundNet, we did not consider it necessary to adopt SWIFT messages, because no local participant used SWIFT messages. It was only when we launched OSP in 2012 that we had to start converting messages into the ISO 20022 format because we were connecting our users to international banks that used SWIFT.

Kech: There are now three passport schemes in Asia: the China-Hong Kong mutual recognition scheme (MRF), the Asia Region Funds Passport (ARFP) and the ASEAN Collective Investment Scheme (ASEAN CIS). What is the state of implementation of the passport schemes in your country, in terms of regulatory changes and automation initiatives?

Prajogo: Indonesia is not, at the moment, participating in any of the three passport schemes. However, non-participation does not mean there is nothing to be done. We observe what is happening when passport schemes are adopted and implemented by other countries. At the same time, our regulator is reviewing and amending the existing regulations, and issuing new regulations with the aim of improving the mutual fund industry. From the point of view of infrastructure, we established S-Invest to achieve a better process in funds-related transactions.

Park: Korea signed the ARFP Memorandum of Co-operation (MoC) in April this year, along with Australia, New Zealand and Japan. In line with the MoC stipulation that signatories amend their legal and regulatory frameworks within 18 months, the Korean regulator is now reviewing current regulations. The law specifies at present that orders in Korean regulated funds must be processed via FundNet, which creates a difficulty if the funds are sold outside Korea. So the imminent launch of the AFRP has led to discussion in the Korean asset management industry over how best to automate the distribution of Korean funds in foreign markets, through linkages between FundNet and fund processing platforms abroad. For foreign funds distributed in Korea, OSP already provides a solution.

Sutthiatthasil: In Thailand, we are looking at both the CIS and the ARFP. Like Korea, Thailand has signed the AFRP MoC, and we have up to 18 months from June 2016 to implement new domestic arrangements. Under ASEAN CIS, five Malaysian funds are being offered already in Singapore, and one Singapore fund is being offered in Malaysia. One Thai-regulated fund is seeking approval from the Singapore regulator, and a Singapore fund is seeking approval in

> **"Five or ten years from now, we expect much greater intra-regional flows within Asia, and we see ourselves playing a role in helping the investment community achieve that. We are looking into how we can enhance our coverage and connectivity within the region to enable the passport arrangements to work."**
>
> **- Isaac Wong,**
> **Director, Product Management,**
> **Investment Funds, Euroclear**

Thailand. Other funds have been registered but are yet to be approved.

Chan: The three Asian initiatives are a natural evolution. Domestic markets have grown and players are now seeking a regional presence and branding. This has implications for fund domiciliation and fund service providers, as well as increasing fund choice for investors. It is the start of a long journey that will need commitment, vision and drive. We will need to learn from the early Asian experience too. The ASEAN CIS entry threshold of US$500 million, for example, may be too high, especially when it is compared with the RMB200 million threshold for China funds in the China-Hong Kong MRF. But passports are definitely a step in the right direction for investors, fund managers, distributors and service providers.

Wong: At the moment, most of our cross-border business is helping channel investment into international funds domiciled in major cross-border centres such as Ireland, Luxembourg and Cayman. Five or ten years from now, we expect much greater intra-regional flows within Asia, and we see ourselves playing a role in helping the investment community achieve that. We are looking into how we can enhance our coverage and connectivity within the region to enable the passport arrangements to work. It would definitely help to have more business-friendly regulations. This is particularly important for the ARFP, because it is the most regional and inclusive of the three arrangements, and still at the formative stage. Another interesting possibility is a mutual recognition agreement between China and any one of the countries in the European Union (EU), or United Kingdom, so Chinese investors can invest in European funds and European investors in Chinese funds.

Kech: There is a trend in Asia Pacific that we do not see elsewhere, of financial market infrastructures (FMIs) helping domestic markets sort out the automation of their funds business. Why do you think that is the case in Asia, what is the current state of your own fund platform, and what are your future plans?

Prajogo: As a self-regulatory organisation, KSEI always looks to participate in and contribute to the development of a more efficient capital market infrastructure in Indonesia. Some participants in the funds industry – such as custodians and brokers – are already participants in KSEI, and adding the other two – fund managers and fund distributors - creates an integrated solution for the market. Concerns related to data confidentiality can be managed, since participants recognise KSEI as an independent and neutral party. As funding is required to establish the new fund platform, KSEI has the capabilities to do so.

Park: As I mentioned, we created FundNet in collaboration with market participants. That helps enormously because, when we propose improvements, we get a strong response from the market participants because they want to increase efficiency further. By making order processing more efficient, we do not just provide a service to the asset managers, but help improve their profitability. In that sense, the KSD has a mutually rewarding relationship with its fund market participants.

Sutthiatthasil: The Stock Exchange of Thailand has for many years taken a leadership role in establishing market infrastructures. For example, 15 years ago we launched an Internet trading platform so that brokerage firms can offer the service to retail investors. It started small, but now accounts for more than 60 per cent of retail activity. We want to lay a similar foundation for domestic fund investment, which we think will grow, chiefly because we have an ageing population. Mutual funds will be an increasingly important investment vehicle for both retail and institutional savers, and we like to think that in ten years' time the infrastructure we have built will be the natural place for them to process orders. We are also in a neutral position, so we are well-placed to facilitate discussions among asset managers, distributors and regulators.

Chan: It is not surprising that FMIs play a different role in Asia to that in Europe. In Europe, the development of FMIs was led by the single market policy. From 1993, when the Investment Services Directive (ISD) first liberalised financial firms to access stock exchange memberships and financial markets across different EU markets, there was a focus in infrastructural development on connectivity and inter-operability. In Asia, the focus of the FMIs is more domestic. They step in to improve the competitiveness and capacity of their domestic market. That said, FMIs in Asia are forging cross-border connections, but it is by asset class rather than by policy – in this case, the connections being forged are between domestic fund markets. Regional forums like AFSF play a key role in facilitating this communication between FMIs and, in the process, are creating a degree of transparency into the market risks, so that investors can better manage them when they invest in Asian markets. That transparency is important because FMIs, such as CSDs, play an important role in mitigating risk, and so help build confidence among global investors.

Wong: As an international CSD (ICSD), we welcome the contribution of the local CSDs in putting the whole funds community together in one place. We share that vision. As a global player, our contribution is to link funds markets to funds markets, and that means being highly

adaptable and connected. In Europe, for example, funds settle in CSDs in some markets, such as France, while in other markets there is a more complex, tiered model consisting of transfer agents and banks. We support either model, but it is obviously more costly to maintain multiple connections. The beauty of a local CSD is a single point of access through one connection. Here in Asia, we would like to help the local CSDs make efficient international connections.

Kech: The AFSF has come up several times. Why does your organisation support its work and what should its role be?

Wong: The AFSF helps the whole community achieve higher efficiencies, lower risk, and lower cost, more quickly. It is a place for us to share our experience from Europe and other parts of the world, and to learn from the local expertise here in Asia.

Prajogo: The key success factor for automation of the funds industry depends on the engagement of the market participants. The AFSF, however, is a good forum to learn from other markets about the current state of their own automation projects, the ingredients of success, and the challenges that remain. All that information is helpful to us in Indonesia, because we are in the early stages of establishing our platform.

Chan: The AFSF brings together experts from each country who know their domestic funds businesses. We are a customer of the CSDs, and at the AFSF we can communicate to them our views on operational and other risks, so that they can be resolved. This helps to build a more resilient and competitive industry that is attractive to overseas investors. Asset manager clients of ours welcome the work of AFSF because regional standardisation helps reduce operational risk and increase productivity. That said, it is important to focus first on the domestic building blocks before we seek to advance on connectivity and inter-operability between domestic fund platforms.

Park: With the expansion of cross-border fund flows in the region, and the three fund passport initiatives, automation and standardisation of post-trade fund processing is more important than ever. There is also a mood among Asian CSDs that fund processing is an essential service for CSDs to provide. This is why we have seen fund processing platforms emerge, such as our own FundNet, the CSDC Central Data Exchange Platform, the TDCC Fund Transmission and Payment Service and the HKMA CMU Fund

Order Routing and Settlement Service. It is also why, when KSD proposed a new consultative body on the standardisation of fund processing at the Asia-Pacific Central Securities Depository Group (ACG) meeting in China in 2014, it was welcomed by the CSDs of the region. The AFSF was launched in November 2015, and we currently have 13 CSDs from 12 economies participating as regular members, and five global fund service providers contributing their expertise as advisory members. The output of our knowledge-sharing workshop in Seoul in June this year is now being turned into an Asia Fund Market Report, and we are working with the Asia-Pacific Financial Forum (APFF) to help fund market regulators in the region understand the importance of standardisation to the success of the passport schemes. The AFSF continues to study various fund transaction models in the region, and we will eventually publish our view of the optimal fund processing model for Asia.

Sutthiatthasil: We are building a fund platform, and there is no better forum for us to learn from the leading experts in the region and from around the world than the AFSF. So AFSF is a must-go-to forum for us. In addition, as fund flows increase, infrastructural investment is going to have to be regional, even global, in nature. If we do not work together now, it is going to be very challenging for us to support the type and volume of business being transacted in the future.

Kech: So what do you think that future will look like? What will the Asian funds landscape look like in 2025?

Sutthiatthasil: Most countries are working on standardisation and automation. This will relieve market participants of the burden of investing in costly infrastructure in the future. Asset managers will be well-positioned to deliver higher returns to their investors. Distributors will not only sell funds at lower cost, but be able to tailor investment solutions to the needs of their clients.

Park: If we project forward the major trends in the Asian funds industry, such as fund passports, increasing investment in funds, and deregulation of the fund industry, we can look forward to an era of border-blind funds. With the ARFP in full swing, and the growth of the ASEAN CIS and the MRF, fund investors across the region will have access to a much more diverse range of funds than those which were available before. The passports will integrate the Asian fund markets, forming a de facto single market in the region. In time, this will generate wealth for investors in emerging markets, rather than exporting it to developed markets. I also expect greater demand for private funds that invest in innovative technology start-ups. To encourage them, the Korean government is already streamlining the regulation of private funds. For all this to happen, fund market infrastructures that adhere to global standards such as ISO 20022 are essential.

Chan: My vision of the future includes the emergence of one or more regional fund domiciliation centres, like an Ireland or a Luxembourg for Asia; the growth of regional funds based on an open distribution architecture that maximises choice for investors; and, as ARFP, ASEAN CIS and MRF develop, that there will be some interest from Europe in making it easier for investors in Europe as well as Asia to switch between UCITS funds and ARFP-ASEAN CIS-MRF funds.

Wong: By 2025, I hope an efficient fund infrastructure will be in place in every country, so market participants can spend less time on processing and more time on building a creative and productive funds industry that offers investors a broad range of investment choices. I have four other predictions. One is that the funds industry in Asia will grow. The second is that international funds from European fund centres (such as Ireland and Luxembourg) and cross-border fund centres (such as Hong Kong and Singapore) will continue to thrive because they have the skills, people and the infrastructures that served Asia well in the past. That said, my third point is that domestic funds will gain in weight, because the authorities in markets such as Hong Kong, Korea and Taiwan have the ambition to grow their own markets. My fourth prediction is that, five years from now, there will be more bi-lateral mutual recognition arrangements, like that between mainland China and Hong Kong.

Prajogo: The funds industry in Asia will grow. As a result, there are pressures to automate the fund industry to keep up with the increasing volume of transactions. Once an automated infrastructure is established, asset managers will be able to focus more on product development and enlarging their investor base.

"The future of funds hubs" at Sibos

Tuesday 27 September 2016
15.30-16.30
Conference Room 3

MyStandards
Standards made simple

MyStandards – a single, common platform to facilitate ISO 20022 harmonisation for market infrastructures and their communities

Market infrastructures

- are driving ISO 20022 adoption

which has emerged as the preferred messaging standard for financial market infrastructures around the world, for securities, payments and treasury business.

- want to achieve a harmonised ISO 20022 approach to ensure a consistent, efficient and cost-effective roll-out for their members

More than twenty-eight market infrastructures (MIs) are already involved in SWIFT's ISO 20022 Harmonisation Framework, which provides a set of best practices around sharing information, adhering to global market practice, introducing alignment around message versions and release cycle management and publishing service information on MyStandards. Since its launch in 2012, MyStandards has become the platform of choice for organisations sharing and publishing their standards specifications.

ISO 20022 In Harmony

ISO 20022 Harmonisation Framework – Stakeholders involved

Payments Markets

Endorsing MIs
Bank of Canada
Payments Canada*
Hong Kong Interbank Clearing
National Bank of Ukraine
Southern African DevelopmentCommunity (SADC)*
ACH Colombia

Additional MIs part of ISO 20022 MI summit group
Bank of England
Reserve Bank of South Africa
EBA Clearing
The Clearing House (TCH)
Federal Reserve Bank, New York
Australian Payments Clearing Association (APCA)
Banca d'Italia
Deutsche Bundesbank
European Central Bank (ECB)

Securities markets

Endorsing MIs
ASX*
Clearstream*
Euroclear*
London Clearing House*
NSD Russia*
Ukrainian National Securities and Stock Market Commission
VP Lux*
VP Securities Denmark*
VPS Norway*
SGX*

Additional MIs part of ISO 20022 MI summit group
DTCC*
Jasdec*
National Bank of Belgium
Deutsche Bundesbank*(as part of 4CB)

FX markets

Endorsing MIs
CLS

* = already published ISO 20022 information in MyStandards

My Standards: a central source for all ISO 20022 information – benefiting market infrastructures and financial institutions

- Increased transparency

Each MI can publish general information about the ISO 20022 messages it uses, its adherence to global market practice as well as its service timetable – on its own public MI page.

- Increased consistency

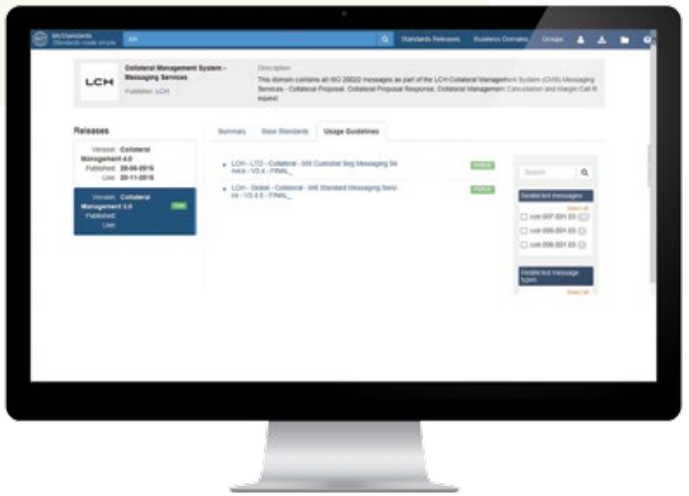
MIs can publish their detailed message specifications in a consistent, high-quality format, including online and downloadable views suitable for analysts and developers.

- Convenient and centralised access to valuable information

MyStandards provides a detailed overview of global ISO 20022 usage, enabling MIs to stay informed and align with best practice when preparing their implementation plans. Financial institutions can easily compare the information shared by FMIs, facilitating efficient impact analysis and better planning.

"Participating in SWIFT's ISO 20022 Harmonisation Framework and using MyStandards to share and publish information (about our ISO 20022 usage and market practices) provides our members and their clients with an efficient process, enabling greater clarity and consistency across the community."

- Gerard Smith, Director, Collateral Services, LCH.Clearnet Ltd



Contact your SWIFT account manager for more information or send an e-mail to **iso20022@swift.com.**

Towards a single payments platform

MI FORUM 2016 | GENEVA

The worldwide shift to real-time payments is irreversible. The important question is whether the payments industry can migrate to a real-time future that combines the safety and soundness of legacy payments infrastructures with the speed, innovation and service of increasingly powerful digital technology. The path to a workable and stable real-time payments industry will be determined by the responses and interactions of incumbents, new entrants, customers and regulators, says Lisa Lansdowne-Higgins, Vice President, Card Operations and Supplier Management at the Royal Bank of Canada, but she believes they all have a stake in a new paradigm that combines the best of the old as well as the new.

The pace of change in payments services is accelerating so rapidly, it is no surprise that we are now entering the era of real-time payments. The journey to this point has certainly not lacked interest. Among the many factors driving real-time payments forward are demands for greater transparency, the need to widen financial inclusion, growing competition from non-banks, regulatory pressure, and of course the growing coincidence between the speed of technology and consumer demands for faster payments.

Real-time payments is now a top priority in every market. Almost 40 countries have committed themselves to achieving it already. Between them, they represent 75 per cent of all payments processed by automated clearing houses (ACHs) around the world.[1] This means real-time payments are now closer to mainstream than ever. In fact, market participants in several countries now view real-time payments as tantamount to a new form of infrastructure, which exists primarily to enable competition between innovative payment service providers.

Infrastructure as an enabler

Faster Payments in the United Kingdom, for example, provides a faster payments service that enables banks to develop a range of competing payments products with many different features. Used in this way, real-time payments infrastructures are not a product or service in their own right. Rather, they act as enablers for other products and services. However, this does present the industry with a challenge. It is to create a new payments eco-system that combines the efficiency and resilience of a market infrastructure with the new product and

1 Gareth Lodge, *Faster Than A Speeding Payment: The Race To Real-Time Is Here*, Celent, June 2016.

service possibilities of technology in a way that is both safe and sound.

The current configuration is a mixture of the old and the new. Payment systems that clear and settle cheques invented centuries ago sit alongside digital systems that clear and settle payments in seconds. The industry has devoted endless human and material resources to the development, maintenance and integration of a multitude of systems that support transactions across a wide variety of "schemes,"[2] each of which operates to different rules and technical standards for executing payments. It is worth asking whether these older methods are still required when the technology exists to settle transactions in real-time.

There must come a point at which the industry ceases to support older infrastructures and migrates clients and payments to their successors. The question we must ask ourselves is this: is there a need to differentiate between settlement streams on grounds of legacy alone? If every form of payment is simply a transfer of value, a single system ought to be able to support every type of payment, while assigning different attributes to each payment according to its behavioural and risk characteristics. This prognosis is consistent with the emerging consensus that a real-time infrastructure can support a variety of innovative "overlay" services.

Current stakeholders will shape the future

Whether this vision of the future is realised depends on the response of incumbents and new entrants, and their customers and regulators, to the challenges and opportunities presented by real-time infrastructures. Their reaction will determine the pace at which payment systems are rationalised, but their response is not entirely under their own control. The wider environment will shape their behaviour, in the same way that external factors have driven the rise of real-time payments to the current decision point.

For a start, the development of real-time payment systems has advanced in tandem with regulatory moves for open access to the payments markets by non-banks. Unencumbered by legacy systems, non–banks are inevitably nimbler than incumbent banks. They can alter the structure of the eco-system by offering innovative services that are more relevant to the retail and corporate customers of the digital age. New entrants rarely

2 "Scheme" is payments industry shorthand for a collection of business rules and technical standards for the execution of payment transactions within a particular community.

> **"Incumbents may find they are better able to compete by migrating to fewer platforms."**
>
> **- Lisa Lansdowne-Higgins, Vice President, Card Operations and Supplier Management at the Royal Bank of Canada**

compete head-to-head with incumbents by offering traditional forms of payment. Instead, they focus on the entire client experience, and look to bundle various components in ways that impress potential clients with their desire to build a relationship with the customer.[3]

A gradual rationalisation of payment platforms

For incumbents lumbered with legacy payments systems, access to ACHs and real-time gross settlement systems (RTGSs) was once a major competitive advantage. It might now be viewed as a handicap. Incumbents find themselves juggling a multiplicity of legacy payments types and services. Rather than continue to do so, incumbents may find they are better able to compete by migrating to fewer platforms. By eliminating the inefficiencies that stem from operating multiple payment systems, incumbents will be able to streamline their operational processes, which will in turn enable them to lower their costs.

But this transition cannot be accomplished by simply closing existing payment systems down. Instead, incumbent banks need to buy time to compete effectively with new entrants. One way to do this is to steer payment volumes to newer platforms by highlighting their service benefits. By this means, less economic methods of payment will run their natural course. Simply put, incumbents need to continue to invest in newer payment methods, while allowing older services to be wound down. It is a solution which provides customers with a choice over how and when to transition their business to a new platform, while allowing incumbents to maintain support for long-established relationships.

The cost of investment in new methods of payments may even fall over time. Real-time payment systems are already being developed in a more modular and flexible way that allows infrastructures and their users to adopt new features quickly and add scale easily. New approaches, such as those promised by distributed ledger technology (DLT), might accelerate the realisation of these benefits still further. In fact, the rapid pace of change in technology, and the growing ability of technology to support new tools, is one of the strongest arguments for the rationalisation of payments systems.

Conflicting customer expectations

In choosing the timetable for rationalisation, customers present incumbents with a dilemma. Their response to the availability of real-time payments is far from uniform, but it divides into two main categories. First, a significant group of customers want the benefits of new technology to be reflected in the payments services they buy. They expect payments to be easy, convenient and immediate. At the same time, another sizeable group of customers are not yet ready to part with tried and tested methods of payment.

This obliges incumbents – unlike new entrants, which have no legacy clients - to continue to support a variety of payments systems. This dilemma may well be resolved by the passage of time. As Millennials become the largest segment of the population, customer expectations will converge on a single model: real-time, digitised, always-on, and available 24/7/365. Reliance on older, non-digital types of payment will diminish in line with the changing demography of the world. Eventually, the case for fewer payments systems will become unanswerable.

Regulators want resilience more than competition

The last group of stakeholders which will influence the pace of adoption of real-time payments is the regulators. For them, safety and efficiency far outweigh lowering the barriers to entry to payments markets.[4] Since efficiency – if not safety – argues for rationalisation, regulators can be expected to support a reduction in the number of methods of settling payments. For the same reason, they can also be expected to support further standardisation of payment flows, including adoption of ISO 20022 by real-time infrastructures, new providers of payments services, and incumbents.

Conversely, rationalisation of payments systems creates risks that might give regulators pause. Chief among those risks is the increased operational risk of reliance on a single system for all types of payment. Of equal concern is how best to ensure continued vigilance about cyber-crime, and effective management of cyber-threats as new payment systems are introduced. These considerations will encourage regulators to insist on higher standards of resilience.

But there are commercial as well as systemic reasons to ponder whether a reduction in the number and range of payment systems is a good idea. Will a single platform put the financial services industry in a better position to compete with the new technology start-ups that are disrupting the payments market today? Will the innovation cycle shorten or extend, as all parties begin to compete with each other off a single platform? Customers of payments service providers may resist rationalisation for that reason: it could reduce the intensity of the competition for their business. While almost everybody in payments recognises that the availability of real-time payments means the industry is at a structural turning point, it is important the eventual outcome strikes the right balance between innovation, competition and safety and soundness.

"Towards a single platform for all payments ..." at Sibos

Wednesday 28 September 2016
10.15-11.15
Conference Room 2

3 Gareth Lodge, *Breaking the payments dam*, Celent, November 2015.

4 Stuart E. Weiner, *The Federal Reserve's Role in Retail Payments: Adapting to a New Environment*, Federal Reserve Bank of Kansas City, Fourth Quarter 2008.

What blockchain might and might not do for CSDs

MI FORUM 2016 | GENEVA

At Sibos 2015 in Singapore, an MI Forum panelist likened ignoring blockchain to lying on a railroad track and waiting for a train to come along. A year on, assessments of the technology by the senior management of CSDs are more sober than that, argues Virginie O'Shea, Research Director at Aite Group.

Nobody could accuse blockchain technologies of being under-hyped. But there is more to the blockchain phenomenon than marketing pitches and soundbites. Real money is being invested. Aite Group estimates that capital markets firms will spend US$130 million on blockchain – otherwise known as distributed ledger technology (DLT) – projects in 2016, rising to a total annual spend of US$400 million by 2019.

An interesting question is what this means for financial market infrastructures (FMIs) such as central securities depositories (CSDs). Some bold spirits believe DLT is ideally suited to revolutionise the economics of CSDs, whose core business is the delivery of assets against payment, and whose reliability currently rests on reconciliation of centralised ledgers held by the infrastructure and its users.

There is even a view that TARGET2-Securities (T2S), the pan-European securities settlement service now half way through a multi-year transition programme to shift the CSDs of the euro-zone on to a platform first conceived over ten years ago, is arriving just as the technology paradigm shifts to blockchain technologies.

Pilot studies are in progress

CSDs are certainly among the organisations investing in pilot studies of how DLT could transform their activities. How advanced these studies actually are varies widely between their sponsors. None is yet advanced sufficiently to make confident predictions about whether DLT is a technology bubble or a valid means of future-proofing the operational platforms of CSDs.

What we do know is that blockchain technology has escaped its origins in the crypto-currency Bitcoin, and acquired a high degree of respectability in the banking and central banking industries. The Bank of England, for example, announced in March 2016 that it is examining the introduction of a central bank digital currency based on DLT as a means of widening access to its balance sheet beyond commercial banks.

The biggest appeal of DLT for the central bank, however, is its potential resilience in the face of external cyber-threats. The fact that the ledger is not centralised but distributed means multiple copies of it are

available throughout the network. Without a single point of failure, a DLT-based network can continue to operate even if multiple participants - "nodes" is the term preferred by blockchain enthusiasts – are knocked out.

At a time when regulators are emphasising cyber-security - the Committee on Payments and Market Infrastructures (CPMI) and the International Organisation of Securities Commissions (IOSCO) published guidance on cyber-security specifically for FMIs in November last year – the resilience of DLT networks is a major attraction not just for CSDs, but for other infrastructures serving the payments and securities industries[1].

CSD applications of blockchain will be permissioned

Yet a technology first designed to allow anonymous counterparties to bypass the entire banking system cannot be adapted to FMIs without adjustment. In applying DLT to the traditional financial system, the technology is allowed to retain its original personality - a consensus-based, distributed cryptographic ledger system – but with one important modification.

The blockchain systems that support crypto-currencies are "permissionless," in the sense that anyone can use them without being approved, or disclosing their real identity. The majority of the systems being developed by FMIs, on the other hand, will be "permissioned." This means they will identify users as white-listed (or black-listed) through variants of Know Your Customer (KYC) procedures.

Benefits of blockchains

This permissioning confers on DLT systems another benefit with a strong contemporary resonance: transparency. As a distributed public ledger, all of participants in a permissioned blackchain network will have complete visibility into every transaction that takes place, and the counterparty. Moreover, as all blockchain transactions are immutable once consummated, there will be no disputes in confirming the veracity of specific transactions.

In addition, permissioned, public blockchains will actually hold a complete history of all transactions, potentially providing a full, built-in audit trail not just for participants, but for regulators as well. This has prompted the blockchain faithful to propound the idea of a form of "RegTech," in which regulators can peer into markets in real-time and implement regulations by distributing software codes, while market participants populate regulatory reports automatically.

Of course, there remains scope for blockchain networks to remain private and anonymous (or pseudonymous). Concern is sometimes expressed that investment banks could pervert DLT networks into a new version of the "dark pools" that caused regulatory concern in the past. This is a genuine risk, since private ledgers will still confer on their users the benefits of economies of scale and reduced IT expenditure as well as the benefits of decentralisation and anonymity.

That said, another benefit of DLT is greater protection against fraud. Because all transactions in a blockchain network must be openly verified via time- and energy-consuming consensus algorithms, it is much more difficult to defraud other participants.

Translating theory into practice is hard

But at present these benefits and risks are theoretical. The only fully functioning blockchain system is the Bitcoin crypto-currency network. Moving from an existing technology platform to

"CSDs are bound to take a measured and cautious approach to radical shifts in their technology strategies."

- Virginie O'Shea,
Research Director, Aite Group

1 The Committee on Payment and Market Infrastructures (CPMI) and the Board of the International Organization of Securities Commissions (IOSCO), *Consultative report, Guidance on cyber resilience for financial market infrastructures*, November 2015.

a new one is a challenging process even within a single financial institution. Shifting entire groups of CSDs from platforms which work, if not perfectly, to an untested alternative, is a risk of systemic proportions.

A transition from the current infrastructural environment (which consists largely of centralised, and often privately owned, networks) to a series of distributed ledgers would take planning on an epic level. Connecting them to each other, to ensure the requisite degree of inter-operability, might well require agreement on a new set of information protocols and message standards.

So the costs and risks involved in transitioning to blockchain remain real, while the benefits are prospective. Until tangible benefits become obvious, and realisable in the medium rather than long term, CSDs are unlikely to take the risk of a wholesale shift to blockchain technologies. After all, T2S faced years of delays and setbacks, despite support at the highest levels in the European Central Bank (ECB), and even now remains incomplete.

Regulatory obstacles to rapid adoption

In the light of the T2S experience, it would take a bold regulator or central bank to endorse an aggressive shift to blockchain even within one country, as opposed to investing in a low-cost experiment, for offensive or defensive strategic reasons. Regulatory anxiety about the resilience of new technologies will remain a significant hurdle to the rapid adoption of blockchain technologies by incumbent FMIs.

Only four years have elapsed since the CPMI and IOSCO published their 24 principles for the safe operation of FMIs[2], and CSDs are measuring their compliance with those principles, and publishing the findings, which indicate shortcomings. National regulatory bodies are adapting the principles into rules, with a view to improving how their FMIs are managed and operate.

Since the rules also have technological and operational consequences, CSDs are bound to take a measured and cautious approach to radical shifts in their technology strategies. Successful pilot programmes that have proved individual transactions can be settled across DLT networks do not provide a practical blueprint for the industry to move wholesale from its current state to blockchain.

In fact, the lasting benefit of the current hype about blockchain may be not the wholesale adoption of DLT at all, but a broader recognition of the value of networks to CSDs, and of the importance of inter-operational standards to extending them. Network effects are an unlimited benefit which CSDs are well-placed to deliver, and the ability to deliver them is not limited to blockchain.

2 The Committee on Payment and Settlement Systems and the Technical Committee of the International Organization of Securities Commissions (IOSCO), *Principles for financial market infrastructures*, April 2012.

"Innovation in the CSD space: What about new technologies?" at Sibos

Wednesday, 28 September 2016
14:00 to 15:00
Conference Room 3

New securities depository entering Slovak market

National Central Securities Depository (Národný centrálny depozitár cenných papierov, a. s. (NCDCP)) has launched its operations. We interviewed Mr. Ľubor Jenis, the NCDCP chief executive officer, about the new institution's activities.

How is the project concerning the establishment of a new central securities depository currently developing?
Having completed the licensing procedure, NCDCP launched its business operations in June 2016. The new central securities depository was founded as a result of the newly adopted Government Concept of the Development of the Capital Market in the Slovak Republic, and established as a subsidiary of Slovenská záručná a rozvojová banka, a. s. (Slovak Guarantee and Development Bank, largest state owned bank in the Slovak Republic). We seized the opportunity and began by setting up our processes according to the latest EU requirements, regulations and current trends. Since February 3rd, 2016, NCDCP has been connected to the SWIFT system and is actively participating in the European project TARGET2 – Securities (T2S).

What objectives should NCDCP fulfil through its activities?
The depository's primary mission is to strengthen the Slovak capital market on an institutional level, and thus achieve a standard of services comparable with that of developed market economies. We are not bringing new titles or more liquidity to the market, though through our well-set processes and links to other entities we can contribute to an appropriate product and price offer. We maintain a close contact and cooperation with banks and securities dealers to estabilish our position. In order to bring an added value to the Slovak market, NCDCP draws inspiration from set examples by our foreign counterparts.

So what can clients expect of NCDCP?
The new depository provides services on a membership basis, i.e. to its members and accepted legal entities. For securities issuers, the provision of services is not subject to depository membership. Our goal is to meet clients' requirements as closely as possible while keeping service efficiency. Traditional branches have been replaced by new technologies, thanks to which clients can deal with their matters quickly, simply and conveniently. The pillar on which NCDCP has based its operations is the HIS Information System, offering the security and flexibility of operations by allowing service requests to be submitted online.
The My Depository client zone is available to all members at www.ncdcp.sk, where a collection of important policies, instructions and forms can be found. We pride ourselves on the professionalism and pro-client approach of our employees, who guarantee a high standard of the services provided.

The instant payments business case – for banks

MI FORUM 2016 | GENEVA

Banks everywhere are under pressure from customers as well as regulators to deliver an instant payments service that never fails and is available around the clock. The investment necessary to achieve this is substantial, while the returns are less certain. The Dutch banks have committed themselves to delivering an instant payments service open to consumers, businesses and the public sector by May 2019. Inge van Dijk, Programme Manager, Instant Payments, at the Dutch Payments Association, explains how the Dutch banks are going about delivering that promise.

"Consumers and companies should be able to send and receive instant payments (within five seconds) both on-line and face-to-face, 24 hours of the day, any day of the year." This was the bold statement of the Dutch Payments Association, the trade association of the banks, payment institutions and electronic money service providers in the Netherlands, in May 2015.

The Association set its members the goal of achieving this objective within four years. The Dutch project fits with the plans - led by the European Payments Council (EPC), under the guidance of the European Retail Payments Board (ERPB) - to design and build a pan-European instant payments scheme.

A year and a half later, the Dutch ambition is still on track. The majority of members of the Association have committed themselves to offering instant payment services from 1 May 2019. The speed of the payments is also set at a maximum of five seconds, which means instant payments will be at least as fast as the current debit and credit card experience of consumers. In other words, from May 2019, instant payments within five seconds will be normal in the Netherlands.

Dutch consumers and businesses want instant payments

Feedback on the timetable and the implementation plan is unanimously positive, from both consumers and retailers in the Netherlands. Merchants in particular have welcomed the proposed service, because it has the potential to provide them with instant

“The infrastructure must be robust, and have sufficient capacity to support growth in the volume and value of payments - without limit.”

- Inge van Dijk, Programme Manager, Instant Payments, at the Dutch Payments Association

access to the revenues they generate over the weekends, when shops are open but banks are not.

Other likely users that have welcomed the prospect of instant payments are eBay-like on-line marketplaces active in the Dutch market, whose users will be able to make instant peer-to-peer payments; companies that can pay temporary workers as soon as a job is done; and on-line consumers that want to pay instantly for immediate delivery of goods.

Support from business and the consumer is essential, because in the end it is the potential customers that will determine the success or failure of instant payments in The Netherlands. To attract as many as possible, the new instant payments infrastructure will be designed to cater for transfers between any and all parties in the Dutch economy, whether they are consumers, businesses or government organisations. Naturally, this implies that the infrastructure must be robust, and have sufficient capacity to support growth in the volume and value of payments - without limit.

The importance of cultural change

Whether to offer customers instant payments-based products and services is a choice now being considered by many payment service providers (PSPs) – not only in the Netherlands, but in Europe and beyond.

The principal challenge they face is the shift in service mind-set required by instant payments. Moving from making payments within the same business day to providing instantaneous payments necessitates a comprehensive review of the service offering to adapt it to a culture of “always on” and “always-available.”

This cultural change applies not just to peer-to-peer payments between consumers, but also in consumer-to-merchant and business-to-business transactions. Banks are conscious they must create a worthwhile end-user experience, or take-up of their instant payments proposition will be slow and uneven.

However challenging the cultural shift, it is one banks know they have to make. If they do not take committed steps now to deliver instant payment services, someone else will likely do it for them. To retain existing customers, let alone secure new ones, the banks know they must develop and deliver products and services that make good use of the new possibilities created by an instant payments infrastructure and go far beyond the current portfolio of payments products offered by banks.

Technology and operating procedures need comprehensive review

In addition to assessing the impact of instant payments on their existing products, and developing new services to generate fresh income streams, banks have understood that they will also need to control their costs and future-proof the investments they will have to make.

Banks will need to undertake comprehensive reviews of their technological infrastructures and operational processes. Their systems have to work within low latency, 24x7 operating timetables and zero down-time constraints to deliver a minimum of 99 per cent availability.

Demands of this kind mean the impact of instant payments reverberates across their entire payments architecture. Security and identity

“However challenging the cultural shift, it is one banks know they have to make. If they do not take committed steps now to deliver instant payment services, someone else will likely do it for them.”

- Inge van Dijk, Programme Manager, Instant Payments, at the Dutch Payments Association

management, initiation channels, payments order management, payment engines, core banking account management, fraud systems and archiving systems all have to be adapted to the increased speed of payments.

Long-term gains can be secured by consolidating currently fragmented payments applications, processes and platforms, but this requires time and investment, which the business case does not always support.

This is especially true of a marketplace in which technology is changing fast. The fast pace of change in digital banking technology confronts banks with an unenviable choice between moving quickly to take advantage of immediate opportunities and planning for the future, when ideally they would like to do both.

Banks must choose whether to compete or collaborate

It might seem obvious that the members of any banking community developing an instant payments infrastructure should collaborate to develop the "scheme"[1] which will be supported by the clearing and settlement services provided by the infrastructure. However, it is the additional customer services layer that should be the focus of their individual efforts. For PSPs, the service layer is of course a very important aspect of the investment.

In making their plans, PSPs can certainly learn from their peers. A number of instant payment infrastructures are already in operation, so banks can benefit from the experience of the early adopters who have made a success of instant payments. That experience can explain not only the factors that govern success, but those which hamper it.

This prompts an interesting question: how far should banks go in collaborating with each other to develop instant payments services? Banks have divergent opinions on this question. Some are developing proprietary services to compete fiercely for customers. Others have chosen to collaborate, especially in the provision of mass-market services such as peer-to-peer mobile payments. When it comes to planning for success in instant payments, the guide book to success is still being written.

1 "Scheme" is payments industry shorthand for a collection of business rules and technical standards for the execution of payment transactions within a particular community.

"Where is the real-time payments business case?" at Sibos

Thursday, 29 September 2016
10:15 - 11:15
Workshop B

MI FORUM SESSIONS

Cyber-resilience in a changing world

Monday 26 September 2016

Speakers:	09:00-10.00 | Conference Room 2

Moderator:

Richard Dzina
Executive Vice President.
Federal Reserve

Stephen Scharf
Managing Director & Chief Security Officer,
DTCC

Adrian Nish
Cyber Security,
BAE Systems Applied Intelligence

Haster Tang
CEO,
HKICL

EU securities markets transformation - is the glass half empty or half full?

Monday 26 September 2016

Speakers:	09:00-10:00 | Workshop A

Moderator:

Dominic Hobson
Journalist

Edwin De Pauw
Director,
Euroclear

Diane Nolan
Capital Markets; Management Consulting,
Accenture

Niels Olsen
CEO,
VP Securities

Mathias Papenfuss
Chief Operating Officer,
Clearstream

Single market and Capital Markets Union - the future role of Financial Market Infrastructures

Monday 26 September 2016

Speakers:	15.30-16.30 | Conference Room 3

Moderator:

David Wright
Secretary General,
IOSCO

Kay Swinburne
MEP,
European Parliament

Pierre Petit
Deputy Director General Market Infrastructure & Payments,
European Central Bank (ECB)

Werner Steinmueller
Managing Director and Head of Global Transaction Banking and Member of the Group Executive Committee,
Deutsche Bank

Godfried De Vidts
Director of European Affairs,
ICAP

Payments inter-operability across communities and currencies

Tuesday 27 September 2016

Speakers:	10:15-11:15 | Conference Room 2

Moderator:

Jeremy Light
Managing Director,
Accenture

George Evers
IPS Director,
VocaLink

Sylvain Debeaumont
Head of Division Market Infrastructure Management,
European Central Bank

Bernard Wee
Executive Director,
Monetary Authority of Singapore

Simone Del Guerra
Deputy Global Head of Transactional Sales, Global Transaction Banking,
UniCredit S.p.A

The future of funds hubs

Tuesday 27 September 2016

Speakers:	15:30-16:30 | Conference Room 3

Moderator:

Alan Chalmers
Publisher and co-founder of Funds Europe Magazine

Philippe Seyll
Co-Chief Executive Officer of Clearstream Banking S.A., and Head of Investment Fund Services and Global Securities Financing,
Clearstream

Katrina Sartorius
Global Head of FundsPlace,
Euroclear SA/NV

Towards a single platform for all payments…

Wednesday 28 September 2016

Speakers:	09:00-10:00 | Conference Room 3

Moderator:

Lisa Lansdowne-Higgins
Vice President, Card Operations,
Royal Bank of Canada

Anthony Brady
Global Head of Business Strategy & Market Solutions,
BNY Mellon Treasury Services

Andrew Hauser
Executive Director for Banking, Payments and Financial Resilience,
Bank of England

Marc Bayle
Director General, Market Infrastructure and Payments,
European Central Bank

Lorenza Martinez
Director General of Directorate General of Payment Systems and Corporate Services,
Banco de México

Innovation in the CSD space: What about new technologies?

Wednesday 28 September 2016

Speakers:	14:00-15:00 | Conference Room 3

Moderator:

Virginie O'Shea
Research Director,
Aite Group

Angus Scott
Head of Product Strategy and Innovation,
Euroclear SA/NV

Cliff Richards
General Manager, Equity Post Trade Services,
ASX Limited

Robert Palatnick
Managing Director & Chief Technology Architect,
DTCC

Where is the real-time payments business case?

Thursday 29 September 2016

Speakers:	10:15-11:15 | Workshop B

Moderator:

Inge van Dijk
Program Manager Instant Payments,
Dutch Payments Association

Christina Friberg
Head of Cross Border Payment Solutions,
Nordea

Joanne Strobel
Head of Technical Sales and Payment Services,
Wells Fargo

Adrian Lovney
CEO,
New Payments Platform Australia

Steve Everett
Product and Propositions, Global Transaction Banking,
Lloyds Banking Group

helping ideas to make it big

connecting ideas and ecosystems, from small startups to big institutions

swift.com/realworldchange

@swiftcommunity
#realworldchange #fintech

SWIFT