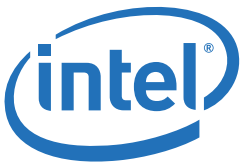
A REPORT ON SIBOS 2018 FROM FINEXTRA
IN ASSOCIATION WITH INTEL
DECEMBER 2018

PUTTING DATA TO WORK IN THE DIGITAL ECONOMY

Finextra



Finextra

FOREWORD

By Mike Blalock,
General Manager, Financial Services Industry, Intel

At this year's Sibos in Sydney, technology and data were again the two key recurring themes identified as critical to enabling and propelling the future of financial services. At prior Sibos events I have attended, technology has also been a key topic, and we reported on the focus around data at last year's event in Toronto.

The difference this year was in two areas. Firstly, the intense focus on integrating technology into the business to save costs and generate revenue especially in the area of advanced analytics and artificial intelligence (AI). How does the industry move from project-based AI deployments to deliver AI at scale dealing with all of the challenges around data to enhance the customer experience, manage regulation and compliance, and enable next generation security?

The second key difference was the concern around global geo-politics – globalism versus nationalism – and its impact on data movement and data access. This is particularly important given that financial services is a global industry based on data. How does the industry balance privacy vs. innovation around the use of data to deliver new services, improve operations and add more value to its customers by enabling data sharing and data exchange across industries and political boundaries?

These challenges and the takeaways outlined in this paper highlight the need and the sense of urgency to develop a new business architecture for financial services that is flexible, adaptable, open and future proof. The business architecture needs to span all aspects of the organisation across infrastructure, data, process, people, and culture, and it will set the stage for data-driven digital transformation.

Open banking initiatives have the potential to accelerate this transformation in most developed banking countries, such as the UK and Australia, allowing new entrants to have access to customer data conveniently and transparently. In this scenario, becoming the customer's trusted data guardian is paramount for established financial services players to succeed. In one session's audience survey during Sibos, 59 per cent of the audience responded that to win in an open banking environment banks should develop utterly new business models. To do this, a new business architecture is needed.

Intel is proud to work with Finextra to provide this report on Sibos 2018 and to be a technology partner for the financial services industry on its transformational journey. We are very excited about this new era of data-centric computing and the potential to re-imagine how financial services are delivered in the future based on technology and data.

FIVE KEY TAKEAWAYS FROM SIBOS 2018

#1: Where open banking is being regulated it is injecting urgency into banks' digital transformation and API strategies, but even where it's not banks are increasingly working with fintechs and other third parties to enhance their business models.

#2: The industry needs to extend its current collaboration and information sharing on cyber risk to stay ahead of emerging threats as well as embrace new tools for financial crime compliance.

#3: Discussion of machine learning and deep learning has moved beyond identifying use cases for trials to operationalising the technology and planning for future advancements in artificial intelligence.

#4: Achieving greater transaction tracking, trust and transparency is a goal shared by technology solutions such as Swift's gpi, and the many consortia projects based on distributed ledger technology.

#5: Cloud technology is now well entrenched and growing. Workload placement and how well financial institutions can quickly select and use the best execution venue across the spectrum of public, private and hybrid cloud will be a key factor in achieving their time to market and cost control ambitions.

KEY TAKEAWAY #1:

Open APIs and banks' transformation to a platform business

Where open banking is being regulated it is injecting urgency into digital transformation and API strategies. But even where it's not, banks are increasingly working with fintechs and other third parties to enhance their business models.

HIGHLIGHTS:

- Australia's open banking regime is being determined by regulation that will ensure customer data ownership and portability across all industries.
- Banks are beginning to see opportunities in business models where they are full service in some areas, but focus on wholesale service provision, infrastructure and data access in others.
- China's financial services market has seen a lot of innovation and competition from non-bank technology firms without specifically promoting an open banking agenda.
- The number of sessions about APIs, and number of attendees at them, at Sibos has dramatically increased, as the discussion has moved away from just being about technical accessibility to one that is driving the digital transformation agenda.

Open banking is a concept notably being championed in Europe, where it has been enabled by the Payment Services Directive 2 (PSD2). At its heart the concept is about unbundling the account and customer data and the financial services that have previously been tightly held by banks, and making them available via API to a wider ecosystem of financial services organisations, particularly in payments.

The Hong Kong Monetary Authority is taking more prescriptive and banking-focused action. It is allowing Hong Kong's biggest banks to pick and choose third party payment providers to work with following its Open API Framework, the first draft of which was published in July 2018.

Singapore is taking a different tack, with the Monetary Authority of Singapore avoiding regulation but fostering an ecosystem of fintechs and encouraging banks to pursue API-based business models.

In China meanwhile, Mike Booth, director of advisory services at Ernst & Young, pointed out that there is no open banking, as such, but they are arriving at a similar place with massively successful non-bank players such as Alipay and WeChat Pay operating their mobile payments services on top of existing bank rails.

But it was the Australian situation that was being most discussed in Sydney as open banking is being driven through regulatory action that focuses on enabling customers across all industries to take ownership of their data. The banks have quite an aggressive timeline to meet the first stage of the Consumer Data Right policy that comes into effect on 1 July 2019. After this date Australians will control their own data and be able to direct the transfer of information between institutions.

There was a lot of interest among international delegates about how the open banking implementation will differ in Australia compared to Europe, and in particular if any lessons may have been learnt from the UK experience.

The introduction of open banking will be phased, starting with credit card, debit card, transaction and savings account data to be followed by mortgage data in 2020. Unlike the plans in Europe, in the first stage customer data will be read-only. But Australian banks expect that write access to customer data and payment initiation could evolve later.

Scott Farrell, partner, King & Wood Mallesons, who led the drafting of the recommendations being implemented as the Consumer Data Right law, told a standing room only audience at Sibos that for everyone attending in a business capacity, the regulation was not about them. But it was about them, and everyone else, as individual consumers.

“The policy is driven all the way down so all Australians have this right. It will go across the entire economy,” he said. “In the review industry kept thinking about themselves. It didn’t matter how many times the word ‘customer’ appeared in the vision statement, I was the only person using it in the meetings. ‘What does your customer want?’ And the response was ‘We want them to want this’. That’s not the desired result.”

Nigel Dobson, Banking Services Business Domain Lead at ANZ, says Australian banks see it as an opportunity rather than a threat. “Regulation helps inject urgency into digital service transformation discussion.

"Banks and payments won't be central to the ecosystem. Payments are just not that important. We will focus on ecosystems for businesses and homeowners. We expect to be visible and branded and front and centre there. But in others we'll be wholesale, invisible but still getting some revenue and importantly, data."

ANZ CEO Shayne Elliott outlined a future for ANZ that include it becoming a more vertical specialist. "In the past the universal banking model was attractive, we would own and operate everything," and aim to add more and more, he said. "But the cost of operations and regulatory compliance makes that less and less sensible for us. So this model is being thrown into doubt." As a result, he says, the future for ANZ would be to do a few things and do them well.

By specialising in a few key areas in a world increasingly embracing open banking models, he expects banks' ability to collaborate successfully in background operational areas – as evidenced by the existence of Swift – to move into the foreground. And this would include not only collaboration with other bank partners but established and emerging technology specialists.

While most of the pressure building for open banking and API-driven business models is affecting the retail financial services sector, the trend is not being ignored by global transaction banking and capital markets businesses.

Claus Richter, Head of TxB Solutions at Nordea, likened possible stages in the open banking evolution to the business models of well-known platform technology companies. The first stage after pure compliance is like Netflix: offering a platform where you sell your own-produced product, as well as that of competitors. The second is like YouTube where you have a platform and you let others monetise it. Finally, the model could become more like Amazon where you sell anything to anyone.

"Banks have to acknowledge we can be leapfrogged and disintermediated, but how deep will we go?" he said. "We can look at today's value propositions and make them more accessible. For example large corporate services through APIs could be made available for SMEs. This could be the first step to a more long-term vision. Next, you need a clear view on where you want to go. As a full bank organisation across all products, you need to get alignment and pursue the vision forcefully."

"Open banking collaboration is an opportunity to have our products enhanced in a more timely way and a cheaper and more efficient way."

PAULA DE SILVA, SEB

SOCIAL SCENE:

@Temenos
'Making the Business Case for **#Payment** Transformation – Lessons from the field' according to the latest **@Ovum report**, banks that delay or defer investment risk falling behind **#OpenBanking #Sibos**

@beelizabeth_
Scott Farrell on open banking at Sibos: "It's not about you" **#Sibos #openbanking #fintech**

@datarepublicans
The open data opportunity is already predicted to generate in excess of $3 trillion in economic value annually across major sectors. Catch **@dannygillan** at **#sibos** talking about this new opportunity

KEY TAKEAWAY #2:

Countering cyber risk and financial crime

The industry needs to extend its current collaboration and information sharing on cyber risk to stay ahead of emerging threats as well as embrace new tools for financial crime compliance.

HIGHLIGHTS:

- Organised crime and collaboration emerging from the dark web are the biggest threat to the financial services industry and our technological society more generally.
- Investment should be more focused on harm minimisation and rapid recovery from breaches than prevention.
- Smaller financial institution partners and non-banks operating in an open banking context are critical weak spots for security that the industry is trying to address.
- For AML controls, transaction/client activity monitoring and customer segmentation are the two main areas that machine learning tools are currently being implemented.

Sibos Sydney 2018 saw the topics of cyber security and financial crime tackled from both a macro and a micro perspective. On the one hand strategic responses and operational models were discussed in relation to the growing pervasiveness and sophistication of threats. On the other, specific solutions for AML and transaction screening were shared, with a focus on how robotic process automation and machine learning based approaches are increasing effectiveness.

“The main threat is coming from organised crime on the dark web,” said CEO of Russian cyber security firm BI.Zone Dmitry Samartev. “Not governments, not from terrorists or hackers.”

The shape of that threat could take many forms. Independent security consultant, Troy Hunt, suggested three main scenarios for a potential 'cyber 9/11': a pervasive and widespread outage of digital services from the internet through to messaging platforms; an attack on professional services including businesses and the banking and financial systems; and attacks on critical infrastructure including power plants and nuclear facilities.

In an audience survey during the cyber risk keynote, 79 per cent of the audience believed that we would have a cyber 9/11 in the next 10 years.

A call that was repeated throughout security oriented sessions was that you can't focus too much on prevention. Instead, it is better to assume you are already compromised or soon will be and instead focus on risk mitigation and harm minimisation. Another view on cyber security strategy is that banks just need to make it expensive and resource intensive enough to compromise their systems that the profit margin for organised bad actors is reduced to the point it is not worth their while.

"No matter how good the technical controls we build we've still got this organic human matter," said David Pegley Managing Director Australian Financial Crimes Exchange Ltd.

"This is about risk management. In exactly the same way we are all now far more accountable around workplace health and safety, we need to be far more accountable around cyber risk," agreed Dr Maria Milosavljevic, Chief Information Security Officer, NSW Government.

But that human element – and the ability to collaborate, share information and work together in creative ways – could mean the industry response eventually becomes more effective than just having banks build higher walls in isolation.

This will mean not just collaboration between large banks. It will also encompass the telco and technology sectors, as well as bringing the smaller financial institutions into the fold and helping them improve their cyber security awareness and processes.

The need for this was particularly spotlighted in the weeks after Sibos, when the Pakistani Federal Investigation Agency's cybercrime wing reported that data from "almost all" Pakistani banks was compromised in a recent security breach, with more than 100 cases being investigated.

At Sibos, Swift announced a specific tool that can help smaller institutions at a transaction screening level. Its cloud based Payment Controls in-network alerting solution for smaller financial institutions can flag, hold, release, or reject high risk or uncharacteristic payments.

Kathryn Taylor, Cyber Policy Initiative at the Carnegie Endowment for International Peace, shared some initial research her organisation is doing into the security practices of small financial services institutions that are not connected to Swift, but may be connected to other financial institutions that are.

"Smaller organisations are the weakest link in financial services system attacks," she said. "We are trying to introduce practical measures and bring the longtail up to speed and make them secure by giving them advice and structures that will work."

But in the meantime, Taylor said that in many cases it is simply an issue of awareness level and prioritisation within these small financial institutions. "If we can get feedback from the industry on the best frameworks and practices to share with them, that will help."

In correspondent banking, financial crime compliance teams are quite mature in the controls and processes they have in place, even if for many organisations manual processing still predominates. But technology is beginning to change this.

Just before Sibos the Institute of International Finance (IIF) released a report based on a survey of 59 financial institutions on their exploration and adoption of machine learning techniques in AML. It found that transaction/client activity monitoring and customer segmentation are the two main areas that machine learning tools are currently being implemented.

This follows the success that many organisations have had in reducing cost over the past year or so introducing robotic process automation (RPA), which has helped to take labour out of processes, and curtail the explosion in headcount within AML departments. For example, Andrew Hoffman, Bank of Montreal, said his organisation had taken out $2.5 million in costs from his AML department through the use of RPA.

Other discussions at Sibos focused more on the retail end of the payments market, and asked what financial crime compliance controls are possible in a world where real-time payments and open banking are converging, and they find themselves dealing with third-party payments providers?

David Howes, group crime compliance, Standard Chartered, said the underlying risk is not dissimilar to correspondent banking relationship. “But if you try to establish that control framework for this space, you’ll realise the cost and difficulty would halt growth. Also it’s probably disproportionate given the values involved.

“Our role is to educate and build programs for nonbanks. Introduce them to requirements of the regulated sector and get them to have the right framework in place.”

“As long as we’re using paper in the trade finance supply chain the opportunities for fraud are immense”
MIKE LIM, ANZ

SOCIAL SCENE:

From @Sibos 2018. Cyber security and geopolitical risk are two major challenges that global banks are facing... “What keeps me awake in the night is not jet lag but cyber” said Gottfried Leibbrandt, CEO, Swift. #Sibos #cyber #cybersecurity #finance #cyberrisk #banksfrauds

Valerie Abend at #Sibos: People are still the easiest target in a cyber attack and the weak link in #cybersecurity – education, awareness and closing gap on skill shortage are key. #embracedisruption

@Innotribe: Securing the future state @JaneFrankland, Cyber Security Capital, explains why including women in #cybersecurity makes us more secure. Women are not better than men, we are just better when we all work together. #Sibos 2018 Sydney Securing the future state

KEY TAKEAWAY #3:

Operationalising machine and deep learning

Discussion of machine learning and deep learning has moved beyond identifying use cases to operationalising the technology and planning for future advancements in artificial intelligence.

HIGHLIGHTS:

- Proofs of concept will continue for ML applications, but focus is also shifting to scale up the areas where it's proving most valuable.
- Data challenges persist, but technology and approaches are being developed to virtualise data sources and
  run models against separate data sets yet return similar results as if they had been merged.
- Graph theory and network analysis models are proving useful at reducing false positives in AML system alerts.
- Lack of expertise is holding back many banks in embracing AI more fully, but leading banks are investing in training and developing education pathways for the roles they will need in future.

Advanced analytics and artificial intelligence was a dominant theme at Sibos, from the futurists talking about the potential of generalised AI sometime before 2050, to the bankers and technologists who are today implementing and benefiting from machine learning (ML), deep learning and associated tools.

"Technology has always been important, but at Sibos this year more than ever it's about really bringing it into operational and business processes," said Mike Blalock, General Manager Financial Services Industry at Intel. "Specifically AI is coming down from the ivory tower proof of concept stage and being integrated into our business processes with all the data."

There are many use cases for technology that sits in the AI spectrum but more are continually being proposed. The main ones currently include:

- Churn prediction
- Customer service optimisation, particularly around voice platforms
- Process optimisation
- AML screening and controls
- Cross and upsell, and customer resurrection
- Marketing personalisation

But for all of them, data is a key requirement. Ramneek Gupta, Managing Director and Co-head Global Venture Investing at Citi Ventures, said a major problem is that lots of data is still not usable. “There is an eternal silo problem. Data lake initiatives have been going for the past five years. But we’ve ended up with multiple puddles not lakes. It’s not an issue for Facebook and Google, which were built around centralised data infrastructures. Financial services and enterprise are not in the same boat. So we’re trying to do virtualised data lakes, a data fabric that virtualises access to resident data everywhere for ML processes with permissioning rules and other requirements.”

There are multiple approaches to handling the data challenges. Some automation is possible in areas such as data labelling, but there was almost universal acceptance across the various keynotes and panel discussions that people with domain expertise will continue to play a critical role in overseeing and bringing that data to life for the models to use.

“Automating data processes is one of the major challenges to overcome in order to scale,” said Parviz Periavi, Principal Architect, Intel. “Secondly, automated model development and serving is another area that enables larger implementations. Lastly security, if you’re using AI as a black box, how can you trust the outcome and trust the security has been taken care of and there has been no tampering? In some of these challenge areas technology and solutions exist today. In others it’s still coming along.”

Lisa Frazier, head of the Innovation Group at Wells Fargo, spoke about the benefits of having a centralised AI team, and how they overcame the organisational difficulties of moving AI projects from small proofs of concept to useful live implementations.

“We had found that earlier POCs didn’t seem to go anywhere. Partly because business awareness about AI was low, but also because there was little thinking about processes and the path to live,” she said. The bank also found that it had tech teams in different lines of business doing very similar things but with different vendors.

"We changed the structure and moved AI under innovation. But it's not just toys and labs. We incubate to live for a number of years before a project grows up to get its own department and cost centre."

Having consolidated vendors and focused its attention on a few particular business problems, the AI group is now working mainly on personalisation, fraud prevention and conversational AI voice as a new platform. "This one will be important," she said. "Today 20% of mobile internet searches are voice. But that will be 50% by 2020."

Another advanced analytics and AI use case that got a lot of attention at Sibos was in AML controls. Current rule-based approaches to transaction screening generate a lot of false positives, and these all require manual investigation. Some banks report that up to 95% of their rules-based alerts are false positives. By improving accuracy through AI, they can reduce the overall number of alerts, improve the rate of alerts reflecting truly suspicious activity, and reduce the time spent on pointless investigation.

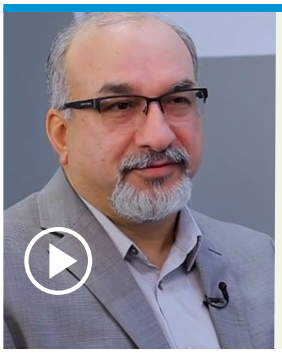
The models that are successfully being used for this are based on graph theory and network analysis. These models can check the network measure of distance links removed between counterparties across massive sets of transaction history. They don't require any additional information about the people or companies or the transaction. But they can be used alongside other different models based on more data points to improve the overall results.

As the technology progresses there will be an increasing demand in the workforce for people who can not only develop AI, but also manage the governance of its models. And this talent supply shortage is already beginning to hit. One Sibos session poll found that 65 per cent of attendees said lack of expertise was stopping them using more RPA and AI to combat financial crime.

But banks are increasingly taking a proactive and collaborative approach to reskilling their workforce and generating the right skills in potential employees. For example, Bank of America Merrill Lynch has had its heads of operations and technology work with universities to develop appropriate courses for the skills the banks will need, including investing in a programme for responsible AI at Harvard University.

Wrapping up the Sibos closing address, Genevieve Bell, distinguished professor at the Australian National University and Senior Fellow at Intel Corporation, provided a thought-provoking anthropological perspective on artificial intelligence and cyber-connected systems – part of the fourth wave of the industrial revolution, and a World Economic Forum diagram from several years ago that has been repeatedly referred to throughout the week.

She pointed out that often, the discussion is based too much on the technology and its capabilities and limitations, and not the wider human and societal impact. She drew an analogy asking if steam engines were the technology that inspired the rail network – which dramatically transformed societies worldwide – what will be the rail network powered by AI? And also, as each wave of the industrial revolution had created new jobs, it also created new areas of academia and applied sciences. From engineers dealing with steam, MBAs with mass production and computer scientists emerging from the digital revolution, she asked the banking industry leaders and technologists in the audience to consider what would be the equivalent created from AI – and what would they need to do to answer questions about safety and scale?



"You do need a consistent high quality flow of data for ML to work. Data discovery, integration and pre-processing are the challenges."

PARVIZ PERIAVI, INTEL

SOCIAL SCENE:

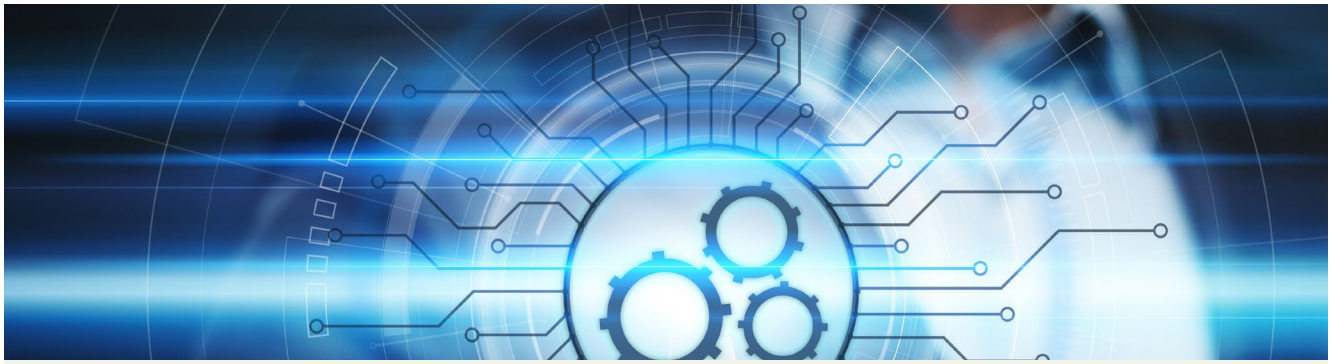
@DuenaBlomstrom
"The machines can have the jobs, us humans will hold on to the talented purpose." TheFutureofWork #Sibos #PeopleNotTech #AI

@kirsi_ripatti
Which area of your life will #AI help out the most? #sibos 2018 #ClosingPlenary audience reply: #healthcare – #banking was the third on the list.

@DanaBrants
#ai definitely holds a promise! Wouldn't we all want our staff to work on exceptional work which creates value to the end user rather than spending time on routine tasks #Sibos

KEY TAKEAWAY #4:

Transaction tracking, trust and transparency



Achieving greater transaction tracking, trust and transparency is a goal shared by technology solutions such as Swift's gpi, and the many consortia projects based on distributed ledger technology (DLT) that are moving closer to implementation.

HIGHLIGHTS:

- Many proofs of concept for DLT in the trade supply chain have been executed, involving financial institutions, importers and exporters and logistics companies, and these are now moving towards implementation.
- Market infrastructures such as ASX and HKEX are planning blockchain projects in post-trade securities settlement.
- New competitors are building their position as DLT based alternatives to Swift for cross-border payments – the established Ripple, and now IBM has joined the fray.
- Swift's gpi solution for cross border payments has similar aims to many DLT projects – improving the tracking and transparency of transactions as they move from initiation to completion. And through connections to national real-time payment settlement systems it claims to be addressing its speed disadvantage.

This year at Sibos, the many technical consortia that have been formed to formalise standards for distributed ledger technology, along with the consortia of businesses putting into practice to solve particular industry problems, have moved closer to widespread production implementations.

The greatest number of users have emerged for DLT in the trade supply chain, with groups of financial institutions and logistics companies emerging in different markets catering to different trade corridors. While there is some separation between them, there is also a lot of potential overlap, which could lead to future consolidation or partnerships among the groups.

Existing 'bank clubs' operating in the trade and DLT space such as Marco Polo network and we.trade, which have moved beyond proofs of concept, had a strong presence at the event.

Similarly, NTT Data has completed proof of concept phases including 14 Japanese logistics and financial companies, and interoperability with Singaporean and Thai national trade and customs platforms, as part of its plans to create an international trade data sharing platform focusing on Asia Pacific.

NTT Data has been a participant in consortiums such as the Hyperledger group investigating use cases for the Ethereum blockchain since 2016, focusing on the information flow of trade processes, particularly letters of credit and insurance documentation.

But there were also other new groups making announcements.

Voltron, a coalition of banks building a blockchain-based network for automating letters of credit and trade finance documentation, threw open its doors to other banks and corporates ahead of a planned roll out in 2019. Founding members of Voltron include Bangkok Bank, BNP Paribas, CTBC Holding, HSBC, ING, NatWest, SEB and Standard Chartered. Operating over R3's Corda platform, HSBC and ING demonstrated the viability of the proposition in a trial conducted with international food conglomerate Cargill in May this year.

Outside of trade, another emerging area for DLT adoption is in post-trade securities settlement. The Australian Stock Exchange (ASX) presented every day on the exhibition floor about its plans to replace it current post-trade settlement system CHESS with a blockchain based alternative in early 2021, in partnership with Digital Asset Holdings. The Hong Kong Exchange and Clearing (HKEX) has since announced that it is working with the same company to build a blockchain platform for post-trade allocation and processing of northbound trades under the Stock Connect programme with China.

In Africa, the Central Securities Depository (CSD) of Nigeria, and South Africa based Standard Bank, a leading custodian, have successfully completed a pilot using the Quartz Blockchain technology from TCS and Intel for cross-border corporate action information exchange, potentially seeding an innovative pan-African financial ecosystem for cross-border information exchange and transaction settlement.

More contentious uses for DLT were also at the forefront (or back of the exhibition floor) at Sibos. Ripple has been a disruptive element at Sibos for the past few years, setting up its various payment processing technologies based on DLT, and

InterLedger Protocol (ILP) to address interoperability and scalability issues, as a direct competitor to Swift's core business.

Ripple was touting the speed of transactions and rising volume of transactions and participants on its network. But it also had its own fresh competition, not from another new startup, but from IBM.

IBM demonstrated its recently introduced cross-border payments system for financial institutions based on blockchain technology. It is working with Stellar on the product, which converts fiat currencies into digital assets, like Stellar's Lumens – or any other digital currencies or bank-backed tokens – for transmission across the network, with conversion of the digital asset into the second fiat currency completing the transaction.

Swift's gpi, which went live in early 2017, is largely seen as a response to these emerging competitive threats to its cross border payments network. Claiming that the correspondent banking rails are not broken, Swift has overlayed them and added tracking capability and other features available from Swift and third parties, with an API access strategy a key part of the product architecture.

Getting in early to counter the speed claims of its rivals, at the start of Sibos it touted the results of trials of cross-border instant payments using gpi, with gpi banks in Singapore, China and Thailand transmitting payments to Australian bank recipients via Australia's NPP platform in as little as nine seconds.

Swift says that findings from the trial are now being used to finalise a new Swift gpi instant cross-border payments service, designed to scale and integrate with other real-time payment systems across the world.

Discussion about the similar aims of DLT based projects and what Swift's gpi is delivering led Niall Cameron, global head of corporate and institutional digital at HSBC, to admit that "adding a virtual ledger would only increase the ability to track the payment in each step of the process. And APIs could provide notifications to customer and bank all along the journey."

Peter Maddison, executive director at Commonwealth Bank of Australia, said "a solution like this would make payments faster, more flexible and more importantly more consistent, as they do not go through several banks, which each have different banking schedules according to the time zone."

"For blockchain 2016 was the year of the proof of concept. 2017 was the year of the consortium. This year we've seen them move closer to production, bringing those networks to the fore."

MIKE LIM, ANZ

"Cross-border payments is seen particularly by retail clients as slow and expensive. What gpi proves is that it's not rocket science to improve on that. Swift gpi simply puts a transparency layer on how we work as a network."

MARC RECKER, DEUTSCHE BANK

SOCIAL SCENE:

@chatsworthcomms

['Enterprise-ready tokens'] could automate or simplify much of the asset origination, issuance, execution and secondary trading processes that make up so much of investment #banking fees today – @inside_r3's @Mcdtv #Sibos #Blockchain

@BNPParibasAPAC

Bruno Campenon, Global Head of Financial Intermediaries and Corporates at @BNPParibas says that #DLT is an enabler, not a panacea. We need to ensure we are adding value to our clients, their clients and the industry."
#Blockchain #ASX #DAH #Sibos18 #Sibos

@ConsenSysMesh

"It's all about building the standards, building the blocks." @ethereumJoseph #Blockchain #ConsenSysSibos #Sibos

KEY TAKEAWAY #5:

Cloud and the future of computing

Cloud technology is now well entrenched and growing in financial services. Workload placement and how well financial institutions can quickly select and use the best execution venues across the spectrum of public, private and hybrid cloud will be a key factor in achieving their time to market and cost control ambitions.

HIGHLIGHTS:

- Cloud technology adoption is now mainstream in financial services, and organisations are getting more sophisticated in managing it to deliver initiatives faster
- Compute power and data management in the cloud are the building blocks, but increasingly the real value is in domain and technology specific services built on top of them – particularly for projects incorporating machine and deep learning
- As a key enabler for digital transformation initiatives, cloud can actually decrease cyber risk through micro-segmentation and continual verification of security

After years of controversy about whether cloud compute and storage adoption was right for a security conscious and highly regulated industry such as financial services, it is now well and truly part of the fabric for most financial institutions. Digital transformation agendas are pushing the adoption of cloud – in a mix of private, public and hybrid models – wherever there is pressure to respond faster to opportunities and competitive pressure.

Any organisations initiating IT modernisation efforts today need to base them on flexible employment of cloud. It can be public or private on-premises cloud and depending on the requirements for cost, security, and performance the workload needs to land in the right execution venue.

The largest financial institutions will always have requirements for private on-premises cloud infrastructure as part of the mix for dealing with sensitive and regulated data. This is also because they operate at a scale where it is still cost effective to maintain a base of their own in-house infrastructure, while being able to move work rapidly onto public cloud to deal with spikes and new projects.

Polina Evstifeeva, Head of Regulatory Strategy at Deutsche Bank, said the fact that regulators are becoming keen to push the digital transformation agenda means they are more accepting of different IT models, as long as the security and risk management is in place.

"Digital transformation is about managing data – storing and exchanging. Cloud and API models are good for these. Regulators are driving innovation, removing barriers, and are keen to support implementation."

Chat Kapoor, vice president for Google Cloud, said that the successful companies all see technology as a competitive advantage to transform business. "It's easy to justify using cloud for saving money, but if it's time to market that's much better," he said. "Secondly, you can't implement new technology with old rules. Planning cycles can't take nine months. This takes a change in culture and process to address.

"Thirdly, leadership is required because the goal posts will move. For the first, second project and beyond it will change. You need to be able to launch and sustain until you land it. It needs sustained focus. The ones that move very quickly, where they stop thinking about cloud adoption or APIs as projects, but rather as products (with the associated management structure) will be most successful."

Amazon Web Services says it is seeing a sense of urgency in cloud adoption just from looking at its own internal metrics, such as new customers and the increasing number of services its customers are accessing, from compute and storage through to devops and machine learning optimisation.

Swift, too, is evolving its cloud offering. Over the past three years it has made cloud product announcements such as Alliance Lite2, its cloud access gateway, as well as hosted solutions such as Sanctions Screening, and the Correspondent Banking Suite.

This year it has taken that even further – doing a proof of concept to see whether its core messaging solutions can be hosted on Microsoft Azure to enable cloud-native payments, rather than Swift's own physical network and on-site gateways.

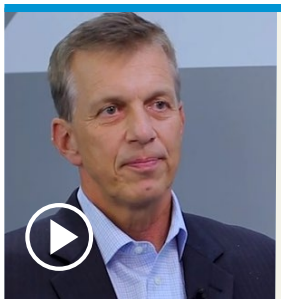
Use cases are expanding, according to Laurence Thiery, Head of Financial Services, Asia, AWS, from high availability serving of retail mobile banking applications through to intensive investment banking operations. "We are seeing use right across the value chain, from wealth management to hedge funds, global investment banks, and even regulators."

Examples given include US regulator FINRA's move of its market surveillance platform to the cloud and National Australia Bank's use of cloud as part of its continuous compliance automation initiative. DBS in Singapore has embraced cloud in its treasury and markets business, for pricing and valuing financial instruments for risk management – something that requires extensive computing power. It has now migrated its Murex solution onto the cloud to take advantage of elastic scale computing power, and it expects to save 70% and is aiming for 90% of its related costs.

Commonwealth Bank of Australia is also making use of hybrid cloud technologies that are allowing the bank to more effectively manage, evolve, and grow its analytics workloads while also reducing operational expenditures.

Mike Blalock, General Manager Financial Services Industry at Intel, said that the growth in analytics and AI requirements in areas such as natural language processing will make it even more critical for all financial services organisations – from banks to fintechs and infrastructures to regulators – to be able to achieve scale quickly on new initiatives.

"A best execution strategy based on performance, price and security across on-premises, private and public cloud enables a unified data platform that gives you the capability to deliver analytics and AI at scale to the entire enterprise."



"A best execution strategy based on performance, price and security across on-premises, private and public cloud enables a unified data platform that gives you the capability to deliver analytics and AI at scale to the entire enterprise."

MIKE BLALOCK, INTEL

SOCIAL SCENE:

@msftfinserv
#Cloud-based solutions are helping banks mitigate risk and remain compliant with new regulations such as #FRTB. Learn more from Day 3 of #Sibos:

@nicholas_redhat
BBVA built a #cloud platform that can be deployed to an entire country in just 4 hours.

ABOUT

Finextra

This report is published by Finextra Research.

Finextra Research is the world's leading specialist financial technology (fintech) news and information source. Finextra offers over 100,000 fintech news, features and TV content items to visitors to www.finextra.com.

Founded in 1999, Finextra Research covers all aspects of financial technology innovation and operation involving banks, institutions and vendor organisations within the wholesale and retail banking, payments and cards sectors worldwide.

Finextra's unique global community consists of over 30,000 fintech professionals working inside banks and financial institutions, specialist fintech application and service providers, consulting organisations and mainstream technology providers. The Finextra community actively participate in posting their opinions and comments on the evolution of fintech. In addition, they contribute information and data to Finextra surveys and reports.

For more information:
Visit www.finextra.com, follow @finextra,
contact contact@finextra.com
or call +44 (0)20 3100 3670

Intel

Intel is a world leader in the design and manufacturing of essential technologies and platforms that power the cloud and an increasingly smart, connected world. Intel technologies unlock the power of data, and our strategy is to provide the technological foundation for the new data world. Accelerate Digital Transformation and Financial Services innovation based on technology and data with Intel.

Additional information:
Visit www.intel.com/fsi, follow @IntelBusiness

Finextra

Finextra Research Ltd
1 Gresham Street
London
EC2V 7BX
United Kingdom

Telephone
+44 (0)20 3100 3670

Email
contact@finextra.com

Web
www.finextra.com