International Securities Services Association

ISSA Symposium 18

24 – 27 May 2016

An Account of Proceedings

By Dominic Hobson

July 2016

CONTENT

Cyber-Crime: A Chief Security Officer View

The following is a summary of key thoughts presented by DTCC's Chief Security Officer:

Cyber-crime is a growth industry. One analysis estimates that the annual losses to the global economy from cyber-crime lie between $475 billion and $575 billion.[1] The unmeasured costs include the theft of personal information. A firm that monitors cyber-crimes that reach the public domain calculates that, since 2005, cyber-criminals have breached the privacy of nearly 900 million personally identifiable records.[2]

Resolving the issues created by cyber-attacks is time-consuming and expensive. One study found the average time taken to deal with a cyber-attack among a benchmark sample of companies in the United States in 2015 was 46 days, and the average annual cost was $15.42 million. The average annual cost to 252 companies across seven countries was $7.7 million, with the real costs to individual companies rising as high as $65 million.[3]

Among the firms taking part in the study, financial services companies experienced the highest average annual cost. At $13.5 million, it is more than twice the equivalent figure for the defence industries in ($6.61 million), nearly three times the average cost to retailers ($4.88 million), and seven times the cost to companies working in agriculture ($1.97 million).

The study found these substantial costs were incurred mainly in disruption to business (39 per cent of the total) and loss of information (35 per cent), but also in lost revenues (21 per cent), damage to equipment (4 per cent) and other costs (2 per cent). Further costs were incurred in detecting cyber-attacks (30 per cent), recovering from them (23 per cent), containing the effects (16 per cent), investigating incidents (14 per cent), managing incidents (9 per cent) and improving cyber-defences for the future (7 per cent).

Cyber-attacks are inspired and driven by a wide variety of reasons, but money and espionage vastly outweigh ideological, grudge-based or frivolous motivations. One study of over 100,000 incidents that took place in 2015 in multiple industries across 82 countries concluded that 86 per cent of cyber-attacks were motivated by either money or espionage, with money alone accounting for four out of five cases.[4]

---

[1] McAfee and the Center for Strategic and International Studies, Net Losses: Estimating the Global Cost of Cybercrime, Economic Impact of Cybercrime II, June 2014.

[2] 899,587,955 records breached from 4,973 data breaches made public since 2005. See Chronology of Data Breaches at www.privacyrights.org

[3] The other countries are Germany ($7.5 million), Japan ($6.81 million), Unite Kingdom ($6.32 million), Brazil ($3.85 million), Australia ($3.47 million) and Russia ($2.37 million). See Hewlett Packard Enterprise in conjunction with the Ponemon Institute, *2015 Cost of Cyber Crime Study: Global*, October 2015.

[4] Verizon, 2016 Data Breach Investigations Report, Figure 3, page 7.

Equally, the study found that most attacks rely on either social engineering (persuading people to open attachments) or stolen credentials (mainly at the point of sale or by using malware to export data). When its analysts examined 8 million phishing emails sent by security vendors to test cyber-defences, 30 per cent of employees opened the emails, and 12 per cent clicked on the malicious attachment, despite attending training and awareness courses beforehand. The median time for the first user of a phishing campaign to open the malicious email was 100 seconds, and the median time to the first click on the attachment was 225 seconds.

This is one reason why it is taking cyber-attackers less time to execute their schemes, while defenders are getting less adept at detecting breaches and resolving them. The same study found that a heavy majority of attacks (81.9 per cent) took only minutes to compromise and take control of a system, while a clear majority of systems (67.8 per cent) took days to mount an effective response.[5] Hardly any attacks take as long as hours to take effect, and phishing attacks and credentials stolen at the point-of-sale can deliver malware or unlock systems within seconds.

Alarmingly, the study noted that the proportion of cyber-attacks that are detected externally rather than internally is also rising. In other words, companies are getting worse at detecting attacks themselves. Any organisation that relies on third parties or law enforcement agencies to notify it of cyber-threats to its systems has almost certainly left it too late to thwart incurring losses from the attack, yet the study found that these methods of detection are rising, while internal filters are declining in effectiveness.

These trends coincide, paradoxically, with a rising awareness of the importance of cyber-security, especially in the financial markets. 70 per cent of financial services industry respondents to the most recent survey of systemic risks by the Depository Trust and Clearing Corporation (DTCC), completed in the third quarter of 2015, named cyber-attacks as one of the top five risks they faced. More than one in three (37 per cent) cited cyber-attacks as the biggest single risk to the economy, placing it well ahead of regulation, recession and geo-political problems.

The range and nature of the adversaries certainly makes cyber-risks multi-faceted, and financial services firms need to understand the risks better. The most numerous and persistent adversaries are nation-states and crime syndicates. Nation-states seeking economic, political and military advantage are prepared to wait before launching attacks, which can have a devastating effect on the assets, revenues, competitive advantages and resilience of banks and financial market infrastructures (FMIs).

Criminals, on the other hand, are motivated solely by financial gain, and want to profit quickly. Apart from inflicting direct financial losses, their activities can also damage brands and lead to both regulatory fines and litigation. They communicate efficiently, and share information. The tools used by organized crime include anonymous marketplaces (such as the notorious Silk Road web

[5] Verizon, 2016 Data Breach Investigations Report, Figure 7, page 10.

site) and card forums (where credit and debit cards and personal information are trafficked).

By comparison with cyber-attacks launched by nation-states and organized crime, those planned by hacktivists seeking social or political change, or insiders motivated by greed or personal grievance, are much less numerous. However, cyber-attacks from these groups can still disrupt businesses, damage assets and steal trade secrets, with negative consequences for revenues and profits, brand values and consumer confidence. Like criminals, hacktivists and insiders recognise the value of sharing information, and communicating with each other and the wider public.

To defend their businesses effectively against these adversaries, banks and FMIs need to adopt the same methods. In the past, organisations facing cyber-attacks did not discuss the threats they were facing, the events they were investigating, or the incidents they were managing. They assumed their competitors were not facing the same issues, and regarded the sharing of information as a source of competitive and commercial disadvantage.

Today, however, businesses are increasingly willing to share knowledge of the threats they are facing. The stigma of admitting to a cyber-attack has lifted as a result. In fact, companies now maintain a continuous dialogue with both their competitors and their clients. Platforms have emerged, where financial services businesses can share information about threats and vulnerabilities they have detected, and in standardised formats.

In the United States, the National Institute of Standards and Technology (NIST) has published a cyber-security framework. It consists of five functional areas (Identity, Protection, Detection, Response and Recovery), 23 categories (such as Asset Management, Data Security, Detection Processes, Response Planning and Recovery Planning)[6] and over 100 sub-categories. The framework aims to provide a common language for businesses to share information on cyber-security.

In addition to sharing information in a regular and structured fashion, banks and FMIs should also test their controls rigorously. Any control that deviates from agreed tolerances indicates vulnerability. Security professionals should be invited to try and gain unauthorised access to applications, networks and systems, and exploit them.

Independent groups ("red teams") should be formed to challenge cyber-security arrangements and probe for weaknesses. Incidents should be simulated, and war-gamed, and breach response scenarios discussed regularly with senior

[6] The 23 categories are grouped under Identity (asset management, business environment, governance, risk assessment, and risk management strategy), Protection (access control, awareness and training, data security, information protection processes and procedures, maintenance, and protective technology), Detection (anomalies and events, security continuous monitoring, and detection processes), Response (response planning, communications, analysis, mitigation, and improvements) and Recovery (recovery planning, improvements and communications).

management and the legal, human resources, corporate communications, and investor relations departments.

The relative decline in internal detection of threats needs to be reversed. Internal intelligence provides the best means of identifying a breach, and of resolving it before money or information is lost. Anomaly detection and behavioural analysis systems are useful in identifying deviations from normal patterns of traffic. Big Data systems can also be used to ingest large volumes of data and detect when apparently innocuous actions are concealing a cyber-attack.

The purpose of all of these defensive measures is to raise the cost of mounting cyber-attacks. At present, the returns are great and the costs and risks are low. A willingness to share information is vital to transform the present imbalance in the terms of engagement between cyber-attackers (low cost and high reward) and cyber–defenders (high costs and no reward). Changing the terms of the trade-off will deter criminals, if not nation-states.

Transformative Technologies

It remains unclear whether distributed ledger or blockchain technology is genuinely transformative, or over-hyped. However, capital is being invested in it on a noticeable scale. According to McKinsey, investment by venture capital firms in blockchain start-ups has grown at a compound rate of 40 per cent a quarter since the beginning of 2013. Venture capital put $598 million into blockchain projects in the 12 months ending September 2015, and the banking industry is expected to invest $400 million more by 2019.

The consulting firm says it has identified more than 60 potential use cases across multiple industries, but many of the most advanced lie in financial services. McKinsey reckons two in five of its use cases focus on the industry, and 68 per cent of them on cost reduction, as opposed to just 15 per cent on revenue. Payments and post-trade clearing and settlement processes in the securities markets are the principal target markets.

Table 1: How Blockchains Work

As its name suggests, a blockchain is a chain of blocks of transactions. It is because a constantly updated copy of all the blocks in the chain is shared with every member of the blockchain network that blockchains are also known as distributed ledger technologies. So-called "miners" ensure the contents of the ledgers can be trusted by competing to discover unique "hashes" (cryptographically secure sequences of letters and numbers they find by anonymous "proof of work") and attach them to a block of transactions.

Because they must use the hash of the block immediately beforehand to produce it, before adding a block to the chain, "miners" ensure that every transaction is legitimate. Any attempt to change a transaction after settlement would change the hash of that block of transactions, signaling to all members of the network that the transaction was tampered with, because the hash would no longer match the previous transaction. By this means, each block of transactions becomes immutable. A blockchain is merely endless blocks of immutable transactions.

From a book-keeping perspective, a blockchain is more like a journal than a ledger, but because it is distributed to every "node" in the network whenever a block is added, every participant always owns a complete copy of the whole ledger. This increases security, because there is no single point of failure in a distributed ledger network. In this sense, blockchains are a classic Internet technology (the Internet was invented by the United States military to ensure connectivity was maintained even if 50 per cent of communications nodes were destroyed).

Unlike centralised ledgers, where transactions move from bank to bank via clearing and settlement infrastructures and it is left up to the banks to allocate the correct value to the accounts of clients, distributed ledgers do not necessitate the reconciliation of multiple sets of ledgers. Instead, value moves from payer to payee, with all transactions and transaction details written into the one ledger sequentially. This elimination of multiple reconciliation processes is the major source of cost savings in distributed ledger technologies.

Certainly the four functions provided by distributed ledger technologies – the ability to transfer value, identity management or counterparty recognition, and registries of both financial assets and transactions in them – can be applied to a variety of services currently provided by custodian banks and financial market infrastructures (FMIs). They include real-time settlement of transactions, perhaps originating on distributed order management platforms, direct access to central bank money, and know your client (KYC) storage and searches.

However, McKinsey has found few products and services actually live. Of the business models on its list, not one is both fully commercialised and scaled. The two most prominent applications of distributed ledgers in the securities services industry are not yet operational. One is the appointment by ASX Limited of Digital Asset Holdings to re-engineer clearing and settlement processes in the Australian cash equities market. The other is the collaboration between Euroclear and itBit to build a new settlement capability for the London gold bullion market. Interestingly, both projects suggest that collaboration between new entrants and incumbents is important to success.

Impact of Blockchain Likely to Be Large

If they do succeed, and encourage imitation, the effects on the securities services industry could be profound. Analysts at Autonomous Research have estimated that, within five years, distributed ledger technologies could cut $16 billion from the $54 billion spent every year on post-trade clearance and settlement processes. McKinsey argues that the revenue impact of the technology in payments and securities clearing and settlement could be as high as $70-85 billion, and that the earliest impact will be felt within 18 months, and the full impact inside just four to five years.

If these two research houses are right, and the revenues currently enjoyed by custodian banks and FMIs are at risk on this scale and timescale, it is obvious that distributed ledgers will lead to major restructuring within the securities services industry. This will apply whether banks and FMIs lead the innovation (as some think they should) or become mere beneficiaries of its introduction by others (which some think they will).

Either way, given the apparent inevitability of the impact, an important question for custodian banks and FMIs is how to prepare for both the threats to existing revenues and the opportunities to create fresh revenues that distributed ledgers represent. A good starting point is to ask which intermediaries in the current value chain are most at risk of being disrupted or displaced or disintermediated by this technology.

Which Intermediaries Are Most Vulnerable?

McKinsey argues that any financial function characterised by a limited degree of trust, a potentially exploitative natural monopoly, a vulnerability to cyber-attack, ample but redundant processing capacity, and an appetite for time-stamped and immutable data, is well suited to disruption by distributed ledger technologies.

Cross-border cash payments and trade finance share these characteristics. In fact, Mckinsey believes correspondent banks are virtually certain to lose their

cross-border payments franchise to blockchain-based alternative networks. This is because blockchain networks offer lower costs and tighter security than the current correspondent banking networks. Providers affected are likely to include non-bank service providers intermediating remittances.

The still paper-based trade finance industry, on the other hand, will probably benefit from efficiency gains in the form of real-time automation of trade data, shipping, monitoring, verification, submission and fulfilment. The industry could also benefit from adopting smart contracts (to calculate settlement amounts and transfer funds) and creating smart assets (such as placing sensors on physical goods to inform the blockchain nodes of delivery). The repo markets will also gain from reduced counterparty and daylight risk from moving to blockchain, or cleared blockchain, networks.

Table 2: Smart Contracts: A User Case

So-called "smart contracts" have emerged as a useful way of issuing financial assets into a blockchain platform, and trading them on the platform as well. They are akin to legal contracts, but the terms are written in digital code. Whereas traditional trades require the counterparties to agree prices, amounts and other terms, with discrepancies picked up in the matching and settlement processes, smart contracts capture all the terms of both the asset and the transaction, and execute the trade automatically.

As a test case conducted by one bank demonstrated, distributed ledger technology enables issuers of securities, and investors in them, to connect and transact directly, eliminating the need for highly intermediated trading and settlement processes. Both the issue and the distribution to investors of bonds was accomplished using smart contracts to represent the securities ("smart bonds") and the means of payment ("bondcoins").

The terms of the smart bonds – principal, maturity, coupon, and coupon frequency - were set by the issuer, who issued them into a blockchain platform via a web browser. Investors linked to the same platform then published indications of interest (IoIs), and used the asset-backed bondcoins as settlement currency for any IoIs accepted by the issuer.

Once the issuer had accepted an IoI, the investor paid by transferring bondcoins to the account of the issuer. Coupon payments were also made by the issuer in bondcoins, directly to the account of investors, until the proceeds of the issue were repaid at maturity, also in bondcoins. The distributed ledger recorded and confirmed all activities between the issuer and the investors.

The test case raised a number of issues. First, both the smart bonds and the bondcoins had to be stored in escrow until they were used, which effectively meant investors had to pay for the bonds in advance. Secondly, in the blockchain platform, all transactions were visible to both parties, which is not the current practice in the bond markets. Thirdly, at 15 seconds per block, transactions were unacceptably slow to settle because the process relied on "proof of work" algorithms. Finally, the user experience for both issuers and investors was not superior to buying bonds through a conventional web site, making it harder to discern the benefits of using distributed ledger technology for this purpose.

Securities clearing and settlement, on the other hand, have characteristics that make FMIs and banks distinctly vulnerable to disruption by blockchain-based services. Central securities depositories (CSDs), for example, are likely to lose their custody function. On the other hand, they are likely to remain keepers of "golden copies" of certificates of ownership, and will have the opportunity to expand into the digitisation of additional asset classes.

The prospects of cash market central counterparty clearing houses (CCPs) are equally assured, as long as a real-time settlement process facilitated by blockchain technology still values netting (as it might in the repo market). Derivatives CCPs will also continue to be required because derivatives trades are collateralised, and they will be needed to continue to verify and store pledged collateral.

Custodian banks, on the other hand, can expect to experience the same decline in demand for traditional custody services as CSDs, and to interact less with CSDs on behalf of clients. This is likely to prompt further pressure to unbundle fees, putting custodian fees under downward pressure. Ancillary services, such as securities lending and tri-party collateral management, may also move in their entirety to blockchain networks. However, if they survive, custodians and their clients will benefit from faster settlement, and a reduction in settlement breaks and errors.

There is one final role the incumbents are likely to retain. Unlike Bitcoin networks, viable blockchain networks are also expected to be "permissioned", in the sense that an entity or group of entities will be authorised to admit organisations to the network to validate blocks of transactions. This implies that central banks, banking co-operatives or associations, or industry-owned FMIs, are likely to retain a role as "permissioning agents."

Distributed ledgers might even be exploited by established networks such as SWIFT, which has 10,000 users, stable communications networks, a reputation for security and operational resilience, a range of standardised peer-to-peer digital messages, safe data storage facilities, and an effective system of governance in place already. These attributes may prove complementary to distributed ledger-based services.

Some Problems Can Be Solved With Existing Technology

An obvious defensive step to take for market participants concerned about the threat from blockchain technologies is to assess whether a particular problem or opportunity is actually amenable to being solved by distributed ledger technology. Many of the issues in the industry – such as internal databases, customer relationship management (CRM) systems, and data storage - can be solved using traditional database and other technologies. The same is true of many of the opportunities.

This is not surprising in an industry that is heavily dependent on digital technology. Its participants are already under pressure to build new technology platforms capable of interacting securely with mobile devices, realising Big Data opportunities, and exploiting the potential of artificial intelligence, machine learning, robotics and natural language processing. In reality, distributed ledgers

are just one manifestation of a range of threats and opportunities created by the drastic alteration in the price-performance ratio of digital technology.

The Potential Benefits of Distributed Ledgers

Unfortunately, despite the falling price of powerful technology, at present much technology spending by both banks and FMIs is pre-empted by regulatory compliance. This limits what is available for innovation. One of the attractions of distributed ledger technology is its promise of a high return (in lower operating, capital and liquidity costs) on a relatively small investment. These savings are chief among a lengthy list of potential benefits adduced:

- *Reduced capital and liquidity costs*: Distributed ledger technology reduces operational risk, chiefly by shortening the time between trading and settlement, and by reconciling trades automatically from a single source, lowering the amount of capital and liquidity that has to be allocated to settlement risk.

- *Lower operational costs*: In addition to capital and liquidity savings, distributed ledgers can cut post-trade settlement costs directly, by reducing settlement timetables, delays and errors, and especially by eliminating the need to reconcile the ledgers of principals and intermediaries on both sides of the trade.

- *Direct regulatory reporting and disclosure*: Regulatory authorities can become nodes on a blockchain network, enabling them to review transactions directly while obviating the need for regulated firms to incur the cost of filing periodic activity and transparency reports to regulators and trade information warehouses.

- *More effective management of systemic risk*: If central banks and securities regulators can see transactional activity directly, they will in effect obtain real-time access to bank positions and other systemic risk information, enabling them to adjust to crises and alter policy more quickly and effectively, reducing volatility.

- *Automation of the compliance process*: Regulatory reporting forms (such as CPO-PQR and Annex IV) and tax forms could be populated automatically with data drawn from distributed ledgers. New regulations could be added to systems automatically, and be enforced by smart contracts written in digital code.

- *Greater resilience and data security*: The fact that every node on blockchain has a complete copy of the ledger means that there is no single point of failure, reducing the need for banks and FMIs to invest in complex and expensive threat exclusion measures and secondary and tertiary back-up sites.

- *No need for industry consensus:* While in theory almost every problem that can be solved by distributed ledgers can also be solved by centralised databases, history shows it is difficult to overcome industry inertia, vested

interest and resistance to centralisation. Distributed ledgers do not face the same "political" constraints.

- *Automation of trade finance*: The risk trade finance addresses is payment before delivery. In a blockchain supported by smart contracts, all parties – shippers, manufacturers, customers, banks and others – can see when goods have actually shipped, and release funding accordingly. This cuts time to payment, as well as risk.

Obstacles to the Adoption of Distributed Leger Technologies

It would be imprudent, however, to ignore the obstacles to the rapid adoption of distributed ledger technologies. Though there are limits to the applicability of the technology *qua* technology – such as replacing current trading platforms in the equity markets, for example – the obstacles are mainly non-technical in nature. They include legal and regulatory mismatches, the need for agreement on connectivity standards, and political issues within the securities services industry:

- *Short term pain for long term gain*: Despite agreement on the long term benefits, in terms of reduced operating, capital and liquidity costs, the short term gains are less obvious to firms managing to 12 month budgets. In addition, the incumbent service providers naturally see current transaction costs as equivalent to their revenues.

- *Collaboration is essential:* In adopting distributed ledgers, banks and FMIs are conflicted, in the sense they profit from the status quo. The value to them of lower costs depends on network effects, which in turn depend on counterparties moving. The process will necessarily be built on collaboration, including with regulators.

- *Lengthy period of transition*: It is unrealistic to expect blockchain start-ups to displace, rather than collaborate, with incumbents. The incumbents need to maintain business-as-usual even while transitioning to a new technology, so the first blockchain networks are likely to run in parallel with existing systems for years.

- *Security concerns*: There are instances in which Bitcoins were stolen by hackers and, although enhanced security is seen as a benefit of distributed ledgers because all data is encrypted and immutable, it is not impossible to envisage scenarios in which bad actors gain control of access credentials or private keys.

- *Standards are required*: There will be multiple permissioned blockchain networks as well as legacy infrastructures. Their value depends on network effects, which are unachievable unless members of otherwise closed networks can communicate with each other, and that depends on agreement on a standard messaging protocol.

- *Common legal framework required:* Despite de-materialisation, most securities laws are currently based on physical securities held in defined jurisdictions. Establishing how these laws can be applied to tokenised financial

assets originally held in issuer CSDs but now issued into and held on blockchain networks is only now beginning.

- *Speed and scalability required*: Bitcoin blockchain technology is too slow to support current volumes of activity in financial markets. Technical solutions to its lack of speed and scalability, such as taking data off-line, compressing data, or economising on what is transmitted, depend on open source collaboration and are not yet robust.

- *Regulation needs to catch up*: Decentralised blockchain networks conflict with national regulatory jurisdictions. Work needs to be done in all jurisdictions to educate regulators and test whether particular regulations apply to a blockchain network. Clearing regulatory obstacles could slow down adoption significantly.

How Securities Services Firms Can Respond to Distributed Ledger Technologies

Despite these obstacles, the securities services industry cannot afford not to take the opportunities presented by blockchain technologies seriously. Bank shares are trading at discounts to book value, so investors believe the current business model is not working, and are therefore inclined to support a bolder strategy.

In addition, successive rounds of cost-cutting have failed to deliver a return on equity in banking that consistently exceeds the cost of capital – only one bank in four has a lower cost base today than in 2007, according to McKinsey - so more radical cost-cutting measures have to be considered. Finally, if banks do not digitise their operations, there is a risk that the revenue opportunities inherent to blockchain will also be lost to new entrants from other industries, or start-ups.

To help banks develop an effective response, ISSA has formed a working group on distributed ledger technology. Its brief is to identify areas where the technology could improve existing processes and arrangements within the securities services industry, and draw up principles to govern its acceptance by practitioners. The working group is also charged with investigating whether distributed ledger technology is capable of fulfilling the many claims made for it.

To further the work of the group, distributed ledger technologies were chosen as one of the two key themes at the ISSA Symposium held from 24 to 27 May 2016. Preliminary reading was distributed to participants in advance of the event and, after a series of presentations and panels on the topic, six sub-groups of participants were formed. These were divided into pairs capable of discussing different aspects of the same three topics concerning distributed ledger technology.

The first pair discussed the issuing of assets into a distributed ledger, dividing their work between the benefits and inhibitors of issuing into a distributed ledger, and the legal regime governing it.

The second discussed transactional aspects of trading and settling assets in a distributed ledger, dividing their deliberations between trading support and the

values and principles which should govern the adoption and use of distributed ledgers in transaction processing.

The third sub-group explored securities lifecycle events and asset servicing issues arising from the use of distributed ledgers, dividing their discussion between proxy voting and income collection and corporate actions.

The detailed findings of each of the sub-groups are summarised in Appendix II. The recommendations the breakout groups had for the ISSA working group are listed in Table 3 box below.

Table 3: Recommended Roles for ISSA to Play

- Delineate the principles by which distributed ledger networks should operate
- Educate regulators on the risks (such as reduced investor protection) and benefits (such as improved transparency) of distributed ledgers
- Work with a tax authority in a particular market to assess the viability of distributed ledgers to make the tax reclaim process more efficient
- Draw up principles for smart contract management across multiple jurisdictions
- Re-visit earlier work on corporate actions and devise principles for shifting the notification and instructions process on to a distributed ledger
- Establish a second working group to review the legal barriers to adoption of distributed ledgers
- Host a blog on the ISSA web site where members can share intelligence and best practices, akin to pooling information about cyber-threats

Based on the above suggestions, the Working Group will now agree on the concrete next steps. Readers are encouraged to follow the milestones and periodic updates on ISSA's homepage, section *Current Working Groups*.

In addition, transformative technologies as seen by a vendor / technical expert are described in Appendix I. This is a summary of a speech given by a representative of Digital Asset Holdings, New York.

Inherent Risks within the Global Custody Chain

In November 2015 the ISSA Board formed a working group to update its 1992 *Report on Global Custody Risks*. The industry has experienced a great deal of change since 1992, so an updated version was long overdue, on grounds of the passage of time and events alone. The fact that the original document remains the most-read paper on the ISSA web site suggests there is also a public appetite for information about the subject, and a limited number of places to find it.

Following a two day meeting in London in November 2015 to review the original document, the working group decided on a revised structure, and commissioned texts from its members. The result of their collective efforts is a new draft paper on the subject, entitled *Custody Risks: Inherent Risks within the Global Custody Chain*, sent as pre-reading material to registered ISSA participants in May 2016.

Ten Sources of Risk in the Global Custody Chain

The ambition of its authors is not to describe best practice, but to educate the reader in the scope and nature of the risks run by custodian banks. Its emphasis is practical rather than theoretical. To ensure the document was of a manageable size, the risks posed by securities lending, foreign exchange and derivatives clearing were excluded, but the text still covers ten broad categories of risk in separate sections. They are:

1. *How assets are held*: This section covers the advantages and disadvantages of omnibus and segregated account structures for on- and off-book and on- and off-balance sheet holdings of cash, and the holding of securities in omnibus, nominee and segregated accounts at global custodians, sub-custodians and central securities depositories (CSDs).
2. *Asset safety and protection*: This section reviewed the range of threats (fraud, insolvency, operational error, embargos, regulation, legal, political, counterparty, title transfer and market) to asset safety at every stage in the custody chain (investment, execution, trade capture, clearing, settlement, custody, reporting and asset servicing) and how these risks are affected by account structures.
3. *Client on-boarding*: This section covers the complex set of mutual due diligence checks that custodians and their clients must complete at the start of their business relationship to ensure compliance with capital, credit and product suitability tests and fiscal, legal and regulatory requirements such as FATCA and Know your Client (KYC) and Know Your Client's Client (KYCC).
4. *Service-related risks*: This section covers the risks of loss occasioned by operational failures and shortcomings, such as failure to capture trade details, match or settle trades, notify or execute corporate actions, prevent costly buy-ins, collect income or tax claims, protect client assets from insolvency or misappropriation, avoid fines and sanctions for compliance failures, or prevent disruption or destruction of systems.
5. *Credit risks*: This section covers the means by which custodians protect themselves from loss when advancing intra-day or overnight credit to clients to fund settlements, and when they offer clients contractual settlement date and income collection services, though the viability of

different forms of protection such as liens over or pledges of client assets varies between jurisdictions.

6. *Liquidity risks*: This section covers the risk that clients are not able to deliver the cash or securities required to settle their obligations at a CSD, central bank or sub-custodian bank, and how this risk can be mitigated by the pre-funding of accounts, charging for the provision of intra-day credit, collateralisation, and the use of more sophisticated tools for predicting receipts of cash and securities.
7. *Information security risks:* This section explores how custodians can mitigate the risk that confidential information belonging to clients is lost in storage or transit, misplaced by employees, stolen from bank systems by intruders or lost to a cyber-attack, by means such as encrypting data, monitoring systems, training staff, testing physical and cyber-defences regularly, and restricting access to client data.
8. *Information technology risks*: This section examines how custodians can manage the market, reputational and litigation risk of failing to document system upgrades, maintain up-to-date inventories of technologies, test additions to existing systems, ensure there is sufficient capacity to process the likely volumes of activity, and renew incident management and recovery procedures.
9. *Vendor and outsourcing risk:* This section assesses the risks posed by the reliance of custodians on third parties, such as correspondent banks, providers of transaction processing services, vendors to which they have outsourced activities such as proxy voting, and data vendors which supply price and corporate actions data, and how the risks can be managed by better documentation, governance and SLAs.
10. *Regulatory risk and compliance risk*: This section covers the cost of failures by custodians to keep up with changes in law and regulation in the jurisdictions where they operate, leading to penalties, fines and sanctions, licence withdrawals and reputational damage, and how these risks can be mitigated by monitoring of law and regulation, thorough preparation, and systematic implementation of any changes.

On 25 May 2016, at the Symposium itself, four separate sub-groups of participants were invited to give feedback on the scope, purpose and value of the document as a whole, and to give detailed feedback on different sections of the document.

All of the sub-groups offered a verdict on the document as a whole, but each reviewed in detail different sections. The first looked at how assets are held and asset safety and protection; the second at client on-boarding and regulatory and compliance risks; the third at service-related risks, credit risks and liquidity risks; and the fourth at information security risks, information technology risks, and vendor and outsourcing risks. Their suggestions for general and specific revisions to the document are now being considered by the working group.

Financial Crime Compliance Principles

In recent years, custodians and central securities depositories (CSDs) have faced a rising level of regulatory scrutiny to ensure that they are not directly or indirectly holding assets on behalf of criminals, sanctioned states, politically exposed persons and terrorists. Some institutions were fined considerable sums for inadvertent breaches. In short, financial crime has become a major source of regulatory risk within the global custody industry.

It was to help custodians and CSDs mitigate that risk that in August 2015 the compliance working group at ISSA published 17 *Financial Crime Compliance Principles for Securities Custody and Settlement*, which it offered for adoption by organisations involved in the securities services industry. Market participants began to adopt the principles in October 2015, and they are expected to be universally adopted throughout the industry by the end of 2018.

A crucial aspect of any effective system of financial crime detection is transparency into the beneficial owners of financial assets. This has increased the interest of some investors in holding assets in accounts which segregate their assets from those of other investors. In other cases, investors have balanced the benefits of segregation against the need to contain transaction costs and ensure financial assets remain available for re-use in securities lending transactions or as collateral.

The result, in current markets, is a mixed system in which investors' assets are both commingled and segregated, and for a variety of reasons. But segregation is much harder to achieve when assets are held across borders, as they often are in the global custody industry. Irrespective of the degree of segregation, ownership of assets held across borders is always based on contractual claims. Beneficial ownership is always separated from legal ownership, and the legal owners are invariably custodian banks.

In this role, custodian banks are not relieved of the obligation to know the identity of beneficial owners. Just as they are expected to know the source of the wealth of their own customers, so are they expected to know the sources of wealth of the customers of their customers (so-called Know Your Customers' Customers, or KYCC).

Both Clearstream and Brown Brothers Harriman were the subject of enforcement actions by the United States regulators in 2014 precisely because they had failed to conduct due diligence on the registered owners of securities their customers were trading. Fines for this kind of omission are material. In 2014 it was estimated that the major banks of Europe and the United States had paid at least $128 billion to regulators, of which $62 billion was paid by just one bank.[7]

The hidden costs, in terms of reputational damage, legal costs, expansion of compliance departments and time wasted in reporting to regulators and managing the consequences, are high. Worse, blocking a suspicious trade has

[7] Data from Wall Street Journal, Reuters and The Huffington Post, published in The Huffington Post, 8 August 2014.

knock-on effects on other clients and the custodian banks and central securities depositories that make up a global custody network. These knock-on effects can lead to civil liabilities for non-execution of blocked trades. Worst of all, if a second offence occurs, regulators are much less forgiving, of individuals as well as firms.

As Jed S. Rakoff, a district judge in the southern district of New York put it: "The future deterrent value of successfully prosecuting individuals far outweighs the prophylactic benefits of imposing internal compliance measures that are often little more than window-dressing."[8] It follows that banks need urgently to put in place comprehensive transaction monitoring and trade surveillance programmes, and to adapt these constantly to changes in the way criminals, sanctioned states, politically exposed persons and terrorists launder money. Some examples of potentially suspicious transactions are listed in Table 4.

Table 4: Signals that Money Is Being Laundered

- Significant positions in unregulated instruments, including private placements and alternative funds;
- Equities issued where the number of shares in issuance is high relative to the material value of the issuer;
- Debt securities issued where the amount issued is both significantly higher than subscriptions received and high relative to the capacity of the issuer;
- Debt securities issued where the business purpose of the financing does not make sense;
- Repeated attempts to engage potential agents in discussions about a securities issuance whose purpose and features are unclear or relate to financial instruments that are not common on the market;
- Securities issued by offshore companies where the identity of the principal or the beneficiary of the capital is not identified;
- Securities positions, including investment funds which are closely held by a single customer, or by a group of customers who may each be acting for a single underlying client;
- Investment funds with a constant NAV or a NAV which is changed only in round increments;
- Investment funds, especially alternative funds, where the general investment strategy is unclear or obscured;
- Tax reclaims or requests for credit advice confirmations on apparently short entitlements;
- Entitled positions on which no tax reclaim request is received;
- A refusal to identify the underlying beneficial owner of a securities position on request;
- Receiving cash credits from unrelated parties bearing no apparent relation to securities positions or transactions with the custodian; and
- Making outbound cash transfers in favour of unrelated parties bearing no apparent relation to securities positions or transactions with the custodian.

[8] Jed S. Rakoff, *The Financial Crisis: Why Have No High-Level Executives Been Prosecuted?,* New York Review of Books, 9 January 2014.

Most banks are struggling to deal with financial crime simply because they have such large and over-complicated internal structures, with multiple divisions overlaid by an expensive compliance function. As Deloitte pointed out in a report published in 2014,[9] the range and extent of financial crime has become too difficult to be handled by established internal divisions or departments. "An enterprise-wide approach is essential and should leverage new analytical software tools," wrote the authors of the Deloitte report.

In other words, it has become extremely difficult for large financial organisations to always know about the beneficial owners of the transactions they process and the assets they service. Yet a great deal of data – customer service records, tax reclaims such as W8 BENs, CBOs and TINs, narratives in SWIFT MT 54X messages, prospectuses, share registers, and corporate actions notifications and instructions – is available to banks. It would enable bank employees to understand the identities and motivations of many beneficial owners, if they made use of it, and they ought to do that. After all, in the eyes of the law, failing to access and read documents or other information which disclosed the identity of a beneficial owner is no defence against allegations of money laundering.

This is why the *Financial Crime Compliance Principles for Securities Custody and Settlement* focus on offering banks practical advice on how to counter money laundering, terrorist financing, market abuse, corruption, fraud and the evasion of sanctions by a single practical technique: Transparency of ownership and control in custody arrangements. They are designed to become the securities equivalent of the principles which have long served as a practical guide to action in the payments industry - the Wolfsberg Correspondent Banking Principles.

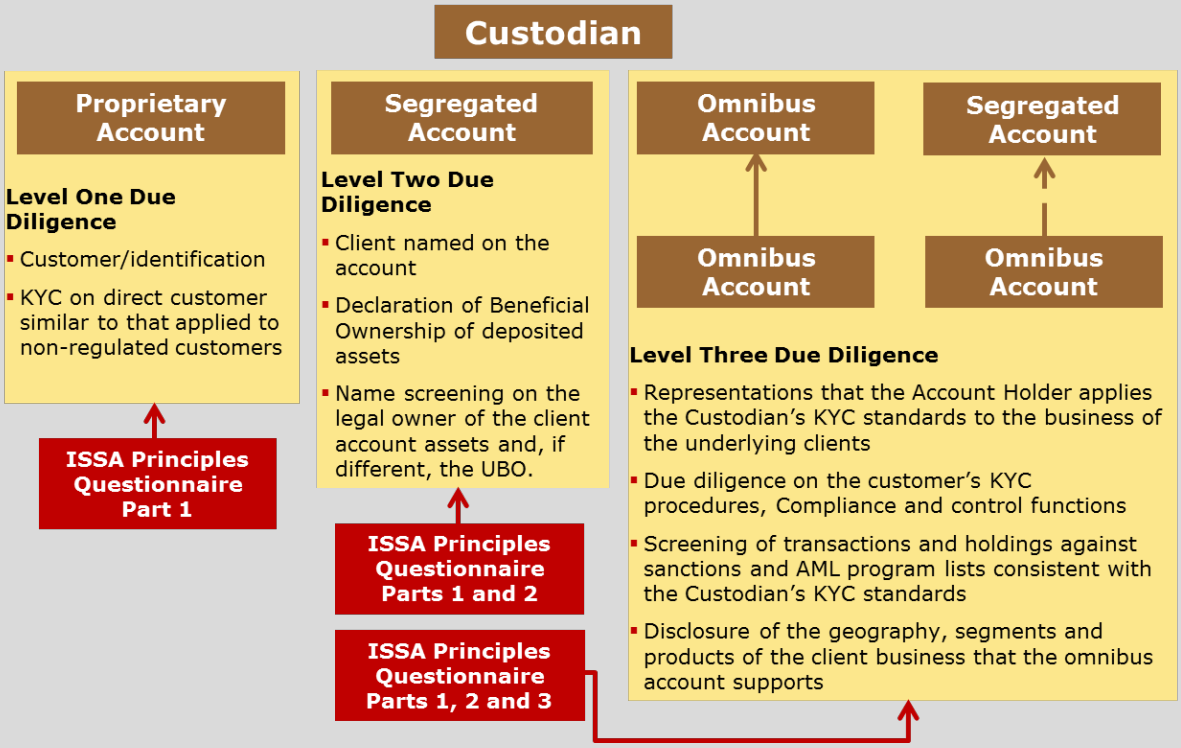
The principles are driven by the new standards that regulators have adopted to address their concerns about the lack of transparency in securities holding chains.[10] It is the responsibility of the custodian bank to communicate the standards it adopts to its account-holders. Importantly, it is the responsibility of the account-holder to comply with those requirements, and to ensure its clients do so as well, and to sub-deposit securities with the custodian only when the beneficial owners have passed a due diligence test.

Putting the principles into operational practice is the next step. ISSA will not monitor adoption by its members, though they are expected to share their progress in implementing them at periodic engagement sessions. Nor will the ISSA principles replace banks' own due diligence frameworks, but Parts 1, 2 and 3 of the principles do provide a checklist of the information required to perform due diligence adequately, using the Know Your Client (KYC) databases that exist already (see Table 5).

[9] Deloitte, *Insight on financial crime: Challenges facing financial institutions*, 2014.

[10] Such as the fourth Anti Money Laundering Directive of the European Union (AML IV), which lays down detailed rules for customer due diligence, ongoing monitoring of customers, and the maintenance of registers of beneficial ownership. The Directive is based on the work of the Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations*, February 2012.

Table 5: The Financial Crime Compliance Principles Due Diligence Framework



Equally, ISSA does not think banks need to invest in additional technology to comply with the principles, and has not proposed a new data standard to "operationalise" the principles. Lastly, the principles do not offer guidance on contractual language to be included in custody agreements either, since it would be a monumental task to cover all jurisdictions represented at ISSA.

However, ISSA is providing guidance to legal drafting teams. The principles that require contractual force have been identified, and the drafting of specimen language is under way. It will be completed by September 2016. Although the specimen language is not designed to replace the work of those banks which prefer to apply the principles using their own legal resources, the specimen language is designed to illustrate to all firms seeking support how to translate the principles into contractual terms.

Once the specimen legal language is published in September 2016, each member firm of ISSA will be invited to appoint a project manager to oversee the implementation of the principles in their own firms. Project managers, co-ordinated by Euroclear, will meet with project co-ordinators at other ISSA member-firms to agree a common implementation roadmap. They will then meet every two months until the end of 2018, when the project co-ordinators will deliver a final implementation report to the ISSA Board.

Regulatory Impact on the Securities Services Chain

The ISSA Working Group on the Regulatory Impact on the Securities Services Chain has published two reports since its formation.[11] In November last year, the ISSA Board mandated the working group to provide members with an update on grounds that, while most of the Group of 20 (G20) requirements are now in place in the major markets, detailed rules are still awaited in many jurisdictions and there are also regional and local variations in implementation.

The initial report of the working group, published in June 2012, sought to understand and predict the impact of regulation on the securities services industry. However, it appeared at a time when most G20 regulatory initiatives were still in their infancy. At that stage, with enabling legislation not always passed and detailed rules yet to be adopted, the report necessarily aimed only to explain the content and objectives of the proposed regulations.

The June 2012 report also highlighted the main goals of regulation: The reduction, monitoring and mitigation of systemic risk; the need for increased transparency to protect investors and monitor the behaviour of market participants; pressure for increased standardisation to reduce operational risk; the ambition to increase competition in financial services by lowering the barriers to entry; and the drive to increase efficiency and reduce costs through projects such as Target2-Securities (T2S).

The report did make some predictions about the likely impact of regulation. It forecast that the volumes of transactions processed by financial market infrastructures (FMIs) such as central securities depositories (CSDs), central counterparty clearing houses (CCPs) and trade information warehouses (TRs) would increase; that banks and insurance companies would continue to play a crucial role as risk absorbers; that costs payable by end-investors were bound to rise; and that a host of new business opportunities would emerge in buy-side outsourcing, collateral management, optimisation and transformation services, and in enhanced reporting services as a result of the pressure to widen disclosure and improve transparency.

The update commissioned by the ISSA Board in November 2015 has extended the near-global reach of its predecessor to include Latin America, but its central aim is unchanged: To examine the impact of regulation on all parts of the securities services industry, including FMIs as well as custodian banks. It will review all regulatory developments since June 2012, with a view to explaining why some regulatory initiatives have changed and others have not. It will pay particular attention to any unintended consequences, and report on how the securities services industry has adapted to regulation so far.

The new report will also take a forward-looking approach in an effort to detect what regulatory challenges are likely to come next, and review the impact on regulation of technological developments such as blockchain and Big Data. Its

[11] Working Group 1, Regulatory Trends and Initiatives Affecting Custodians, Clearers and (I)CSDs: Impacts and Implications, June 2012 and Report on Shadow Banking: Developments of Regulatory Changes and their impact on ISSA Member, February 2014.

approach will be expressly concrete, and illustrated with practical examples, so the text remains accessible, simple and clear rather than long and legalistic.

The overarching goal of the new report is to raise awareness within the securities services industry of new regulations, and to remind participants that regulation remains an important strategic factor in their planning for the future. Ideally, the report will provide a sound basis for anticipating structural changes occasioned by the evolution of regulation and - importantly – help firms understand better the interaction between regulation and other developments, such as distributed ledger technology. To that end, it will address three fundamental questions:

- *First, where does the industry stand in terms of adoption and implementation?* The first section of the report will review pending regulations by region, and distinguish between what is unique to a particular region and what is common to all regions. This will be challenging, because in both Europe and Asia, the G20 regulatory programme is being implemented country-by-country.

- *Secondly, how has the industry adapted so far?* The report will identify the principal impacts, in terms of increased asset safety, greater transparency, a rising compliance and governance burden, and extra–territorial effects, such as FATCA. This section of the report will also look at how the securities services industry has evolved as a result of the regulations, because not all impacts could be anticipated in June 2012. Assessing the impact of each regulation is relatively straightforward, but the report is setting itself the harder task of assessing the overall impact of regulation, and working out how the measures interact.

- *Thirdly, what regulations are coming next?* New regulatory developments include Basel IV, capital requirements for non-banking, systemically important institutions such as insurance companies and fund managers, recovery and resolution plans for CCPs, and measures to tighten cyber-security, which is now the top priority of regulators in the United States. This section of the report will also review the continuing influence on the securities services industry of non-regulatory trends such as blockchain, Big Data and the persistence of low rates of interest.

The working group, which is reliant for information on its regional representatives in North America, Latin America, Asia and Europe, proceeds through regular teleconferences and occasional meetings. The objective is to produce the new report by the end of the first quarter of 2017.

Collateral Management Best Practices

The ISSA Working Group on Collateral Management Best Practices was established to recommend best practices for custodian banks, fund managers and fund administrators engaged in the posting, movement and management of collateral in the securities financing and cleared and non-cleared derivatives markets. The goal of the Working Group, conceived at a time when collateral management was ceasing to be a back office function and becoming an investment management discipline in its own right, was to provide an educational document.

The interim report of the working group, published in March 2014,[12] delivered on that promise. It was informative, but neutral. It was not a sales prospectus for established third party collateral management service providers, but educated market participants on the tools and models available to them to ensure that they always had the right collateral in the right place at the right time to cover the right exposure. The paper also sought to educate regulators. However, the paper could not be exhaustive, or keep up with the rapidly evolving collateral management techniques in the marketplace.

At the 17th ISSA Symposium in May 2014, where the initial report was presented, considerable interest was expressed in the notion of creating virtual collateral pools. This became one of the principal themes of the discussions which preceded the delivery of the final report of the working group, which was circulated to ISSA members ahead of the 18th ISSA Symposium in May 2016. The revised report, which focuses entirely on the movement of collateral across borders, and from an operational rather than trading perspective, also expanded on a variety of regulatory, legal, operational and technical barriers to the cross-border movement of collateral.

Published in July 2016, the final report includes a series of recommendations:

- The need for the industry to maintain dialogue with regulators on the impact of segregated accounts on collateral mobility;
- The beneficial effects of modelling a variety of market scenarios to assess the impact of stressed markets on collateralised funding, including a reversal of the current combination of quantitative easing, plentiful central bank money and low rates of interest;
- Exploration of the value of the collateral and liquidity management standards developed by the contact group on euro securities infrastructures (COGESI) of the European Central Bank (ECB);
- Monitoring of the evolution of infrastructural platforms such as the Correspondent Central Bank Model (CCBM), which is designed to facilitate the transfer of domestic collateral to non-domestic central banks within the euro-zone;

[12] ISSA, *Best Practices of Collateral Management for Cleared and Bi-laterally Traded Products*, March 2014.

- The need to press regulators to adopt a global approach to legal certainty on the posting of collateral assets in cross-border securities financing trades; and

- The development of the case for integrating collateral mobility into broader discussions on disruptive technologies, and in particular to investigate how distributed ledgers could help realise the ambition of a virtual collateral pool on a global scale.

ISSA's Operating Committee has the mandate to evaluate further potential work items by the end of October 2016.

Appendices

Appendix I

Transformative Technologies: A Vendor View

Distributed ledger technologies are a lot less exciting than people pretend. They emerged from crypto-currencies such as Bitcoin, which gives them a risqué reputation, but they are at bottom no more than an ingenious advance on traditional database technology. This nevertheless means the technologies are important, because banks are big users of databases.

At present, banks regard their databases as crucial, but vulnerable. They are concerned chiefly to protect unencrypted databases from being penetrated by third parties. This is why they erect sophisticated perimeter fences around their databases to protect the raw data they contain from intruders.

Contemporary databases also tend to be owned and controlled by a single entity, which retains the sole right to edit the data, including the rectification of errors. Lastly, every organisation in financial services maintains its own proprietary database, necessitating a secondary industry of its own just to reconcile the data held in each of them.

Distributed ledger technologies have the potential to greatly improve this proprietary, fragmented and inefficient collection of proprietary databases. They can create instead a mutualised database infrastructure, in which independent parties can all rely with equal confidence on the same database, because every authorized participant can always verify and validate the data which belongs to them.

In short, the elaborate, resource-intensive, slow and error-prone process of reconciling databases is no longer needed in a distributed ledger environment, because all parties can rely on the same source of information, prove the information is theirs, and be confident it is accurate and secure.

Despite popular perceptions, this vision of the future of database technology is much easier to grasp intellectually than it is to achieve in practice. In effect, distributed ledgers promise a common source of truth – a golden record – to any and all organisations active in the securities, derivatives and lending markets.

If that is not revolutionary, it is still a significant advance on existing practice, not least because it creates the scope to reduce drastically both the costs of post-trade operations (especially reconciliation) and the capital consumed by the current, riskier arrangements.

An important question is how the securities industry can transition successfully from its current infrastructure to the distributed ledger alternative, and why. The attractions include powerful cryptographic techniques, and especially the management of counterparty identities through combinations of private and public keys.

These ensure that the data held on distributed ledgers is much more secure than data held on unencrypted databases. This is because, when third parties cannot

unencrypt the data held on a distributed ledger, every single item of data is accessible only by the parties to the authenticated transaction that the data records.

This characteristic is a mark of the origins of distributed ledger technology in the widespread disillusionment with the prevailing financial system that set in after 2007-08. It was invented to facilitate exchanges of Bitcoins, as an alternative digital currency to the fiat currencies issued by central banks, open to anyone who wished to exchange value through the Internet without the constraints of law and regulation, yielding a cut to intermediaries, or having to trust the counterparty.

The unlawful origins of distributed ledger technology continue to encourage people sceptical of its intrinsic usefulness, those who warn that it will be abused to get round anti-money laundering (AML) and Know Your Client (KYC) regimes, and anyone who believes that central banks should have complete control of the supply of money.

The sceptics are confirmed in their belief by the fact that the original version of distributed ledger technology remains a useful invention in jurisdictions which have low levels of trust, or which lack a properly functioning central bank. But using crypto-currencies to make anonymous payments between counterparties unknown to each other over the Internet is just one application of the technology. In fact – and ironically - distributed ledger technology has multiple applications at the banks and central banks its inventors aimed to bypass. In the securities, derivatives and lending industries, for example, the technology can be used to create a shared database, accessible only by those with a need and a right to read the data.

The data itself is encrypted, and the credentials of the counterparties accessing it are verified by sophisticated identity management systems that also rely on cryptography. In other words, distributed ledger technology makes it possible to verify digitally whether a counterparty is who they say they are, and whether or not they are authorised to access the data. In addition, any item in the database that is changed by an authorised user is immutable.

An obvious use case for these benefits is financial market infrastructures (FMIs). Instead of every participant in the markets running their own post-trade operation, they can share a common, mutualised infrastructure.

This is long overdue. In the front office, intense competition to capture value in the trading of financial instruments means competitive advantage is now measured in fractions of nano-seconds. In the post-trade environment, on the other hand, latencies are still measured in hours, days, weeks, or even months. Latency implies risk, and the longer it persists, the greater the risk.

The potential to reduce that risk, and the costs and capital it consumes, is why distributed ledger technology is relevant to the securities services industry. It is often said that new technologies die if they are looking for a problem to solve. It is better to recognise the problem, and solve the technology.

Fortunately, there exists a post-trade problem that distributed ledger technology can be adapted to solve. Unfortunately, there is a contradiction between the people who understand the technology and the people who understand banking. Many of the technologists familiar with distributed ledgers continue to regard banks as irrelevant or evil.

This contradiction can be overcome. In fact, it must be, because the banking industry is facing serious structural challenges. These originate in a return-on-equity (RoE) problem. RoE is revenue minus expenses divided by capital, and in the banking industry all three metrics are going in the wrong direction.

Revenue is compressed by low interest rates, narrow spreads, and the elimination of proprietary trading. Volatility in financial asset prices no longer helps earnings, because it is driven not by liquidity but illiquidity. Costs are high and rising, chiefly as a result of compliance with new regulation. Simultaneously, regulatory capital is being increased, and will continue to increase for some time to come. Even best-in-class banks are systematically generating RoEs below their cost of capital.

This is an existential problem for the baking industry – and it is why the advent of distributed ledger technology has attracted such a lot of attention. The technology cannot solve every post-trade problem, but it can change materially how transactions are processed, and so reduce costs, afford capital relief, free banks to create and develop new and more profitable services, and make it easier for them to deliver the greater transparency demanded by regulators. This is why every financial institution is now looking at distributed ledger technology.

One effect of this is a degree of hyperbole. Among the many hyperbolic predictions is the disintermediation of brokers, custodians and central securities depositories. Experience counsels caution. In the 1990s, the advent of the Internet created a similar degree of hyperbole. Although it was well understood that the technology was significant, it was impossible to predict the winners. It took 25 years for clear winners, such as Amazon, Facebook and Google, to emerge. The destructive impact of the Internet on the music and media industries also took longer than expected to materialise. The streaming of films is only now becoming widely available.

As the Internet developed, existing businesses adopted, adapted and used it to do business with existing customers. Today, every business needs an Internet capability, or it will be competed out of its markets, but that existential threat took a long time to sting the incumbents. Similarly, banks and FMIs will have the time to adapt to distributed ledger technology, and capitalise on its benefits to lower costs, cut error rates, and share the savings with their customers.

The incumbents are in a strong position. For example, the Depository Trust and Clearing Corporation (DTCC) currently processes 1½ quadrillion transactions a year. It is responsible for protecting title to financial assets, and it is authorised in that work by an Act of the United States Congress. The law will not be changed soon to accommodate new entrants, whether or not they use distributed ledger technology. The opportunity for distributed ledger technology

vendors is not to replace the DTCC, but to engage with it, and see what it could do better.

The time needed for the technology to mature does not mean it does not yet work. Every new technology faces technical challenges, but there is nothing inherently impossible about what proponents of distributed ledger technology are trying to achieve. Several versions are now ready, or being readied, for commercial deployment. However, there remain other obstacles to the adoption of distributed ledger technologies.

Chief among them is the regulatory implications. Although financial services regulators everywhere are excited by the possibility of lower settlement costs, error rates and latency times, they also agree that Bitcoin-style anonymous exchanges are a non-starter. To overcome this obstacle, all mainstream applications of distributed ledger technology are proposing that the "nodes" in their distributed ledger networks be permissioned and credentialised by some form of agreed agent or supervisor. Regulators will also want to eliminate any scope for regulatory arbitrage.

If regulators took powers to act as "nodes" on distributed ledger networks, regulatory reports could become redundant. It helps that rules exist already on how to run a systemically important financial infrastructure, in terms of redundancy, capacity, transparency, privacy, and recovery and resolution. Every distributed ledger technology will have to respect these rules. The technology even offers the regulated as well as the regulators greater transparency, in the sense that the distributed ledgers can hold the details of every beneficial owner of every security in any jurisdiction. This obviates the need to create segregated account structures.

The legal changes required to give effect to these possibilities are minimal, so regulation is unlikely to act as a brake on the adoption of distributed ledger technology. Custodian banks would also benefit from more efficient interactions with regulators. Withholding tax reclaim forms and income tax submissions could be pre-populated with information abstracted from the distributed ledgers. In fact, the technology could in theory render all post-trade regulatory reporting redundant, since the transactions could be seen by regulators at first hand.

A larger obstacle to rapid adoption of distributed ledger technology is network effects. Unless their counterparties are also nodes on the network, allowing banks to exchange value with a significant proportion of their counterparties, the business case collapses. FMIs are an ideal place to start building network effects of this kind because, although financial markets are fragmented, as centres of clearing and settlement they draw participants together through centralisation and standardisation. Many FMIs are also operating with ageing technology platforms, and so have good reasons of their own to adopt distributed ledger technologies, and to extend their benefits to their users.

However, the workability of this approach – in which FMIs encourage their users to adopt distributed ledger technologies – is constrained by the fact that banks are using such old and fragmented technology platforms that they will struggle to close them down and transition to distributed ledgers without damaging their existing business. So any alteration in their technology strategy is bound to be

gradual, but they do have a compelling incentive to change: The prospect of significant cost reductions, without which they may be driven out of business.

Even if they are already investing in new technology, the potential benefits of distributed ledger are powerful enough to prompt a re-consideration. It is entirely possible for a bank to realise some but not all of those benefits, by cherry-picking components, adopting a modular approach, or through hybrid solutions, which combine distributed ledgers with centralised databases.

One final obstacle to be overcome is the risk of banks choosing the wrong version of distributed ledger technology. This threatens them with the prospect of becoming captive to a standard endorsed by few of their counterparties. However, the involvement of the open source community in the development of a cross-industry open standard for distributed ledgers – via the Hyperledger Project[13] - means this is in practice highly unlikely to happen.

In fact, the involvement of the open source community probably marks the tipping point in the adoption of distributed ledger technologies. The first serious commercial applications are now launched. The debate about the applicability of smart contracts has begun in earnest. Vendors of distributed ledger solutions now face serious competition, not only from start-ups and established technology companies, but from in-house technologists. Distributed ledger technologies are still evolving rapidly, but their long term survival is not in doubt.

[13] The Hyperledger Project is supported by six banks (ABN Amro, ANZ, BNY Mellon, J.P. Morgan, State Street and Wells Fargo), two exchanges (CME and Deutsche Börse), two FMIs (DTCC and CLS) and 26 technology vendors.

Appendix II

Transformative Technologies: Distributed Ledger (Blockchain) Technologies

Issuing of assets into a distributed ledger		**Trading and settling assets in distributed ledgers**		**Events and asset servicing in distributed ledgers**	
Benefits and inhibitors	Legal regime	Trading support	Values and principles	Proxies and income	Corporate actions
Benefits: ➢ Faster issuance of financial assets ➢ "Golden source" of corporate data ➢ Real-time updates of stock register ➢ Easier adherence to listing rules ➢ Could solve asset classes other than securities ➢ Transparency into beneficial owners ➢ Portfolio reporting to investors ➢ Direct regulatory reporting ➢ Custodians survive as "wardens" of investor assets ➢ Savings from less reconciliation ➢ Security: no single point of failure ➢ Scope to pick low hanging fruit to prove business case ➢ Distributed ledgers can support both direct issuance of assets and replication of assets already issued into an issuer CSD Inhibitors: ➢ National rules (e.g. CSD access, account structures etc.) too varied ➢ National securities	Benefits: ➢ Distributed ledger captures "golden copy" of data from issuers ➢ Faster, cheaper route to market for issuers ➢ New issue underwriters can use to set prices and terms ➢ Underwriters and brokers can use smart contracts ➢ Transparency for issuers into names of underlying investors ➢ Issuers get direct access to investors ➢ Efficiency and transparency for regulators ➢ Nodes can be identified by existing tags (LEIs) ➢ Ample benefits in asset servicing, notably corporate actions, so could ➢ combine old issuance techniques with distributed ledgers for asset servicing Inhibitors: ➢ Insufficient benefits for issuers to go direct ➢ No incentive for issuers to disintermediate underwriters who market the stock and book-build ➢ Direct segregated holdings already	Benefits: ➢ Settlement systems flexible enough to accommodate multiple post-trade timetables, from real-time settlement to settlement on T+10 ➢ Full transparency into transactions and ownership of assets ➢ Increased security and resilience ➢ Shortens the custody value chain by disintermediating some functions ➢ Distributed ledgers are a useful, capital-reducing, niche solution for inefficient, manual markets such as syndicated loans and private placements ➢ Immediate applicability to emerging markets without legacy systems Inhibitors: ➢ Will not be used for secondary trading, so inefficient linkages between trading and settlement increase the degree of reconciliation ➢ MiFID demands best execution is demonstrable ➢ Need to work across as well as within borders, and there is a lack of	Principles: ➢ Define and demonstrate settlement finality in a distributed ledger ➢ Define how to unwind unsettled trades and counterparty defaults ➢ Ensure regulators have immediate access to all trades of a failed counterparty entering recovery and resolution ➢ Create inter-operability standards between different distributed ledgers and between distributed ledgers and legacy systems ➢ Define due diligence tests before admission to a distributed ledger network ➢ Describe what information in ledgers needs to be made public and what can be kept private ➢ Outline public and private corporate governance structures so users know who is liable and who to appeal to when a problem arises ➢ Decide which entity will act as the "golden source" of records to resolve disputes ➢ Ensure distributed ledgers do not privatise costs and benefits by	Benefits: ➢ Issuers need shareholder approval for many of their actions, and distributed ledgers could enable them to secure that approval more efficiently, perhaps by using the blockchain consensus method ➢ Real problem is not income collection but tax reclaims, and distributed ledger can help with tax because all transactions are recorded on the ledger and tax authorities, investors and custodians can see them simultaneously Inhibitors: ➢ The cost of the status quo may not be high enough to warrant switching to distributed ledgers ➢ Only heavy users of proxy voting are likely to see value in using distributed ledger technology to improve the process ➢ Companies have investors all over the world, and it would be awkward to use distributed ledgers in some jurisdictions but not others, since the pace of adoption is bound to vary	Benefits: ➢ Inter-changeability: a distributed ledger solution for proxy voting would work as well for corporate actions, and vice-versa ➢ Could act as a catalyst to address continuing problems in corporate actions, such as lack of a "golden copy," re-keying of data, and unused and inadequate standards, leading to significant risk for custodians Inhibitors: ➢ Corporate actions still too complex, inefficient, non-standardised, lacking in a "golden source" and heavily intermediated to be susceptible to any technological step change, let alone a distributed ledger solution ➢ The high level of intermediation is not the source of inefficiency but a reflection of inefficiency, so disintermediation is an inadequate basis for adopting distributed ledgers in this sphere ➢ Corporate actions are a sequential process, in

laws need time to catch up ➢ Business case hard to discern yet ➢ Inertia and vested interests opposed to change ➢ IT investment budgets squeezed ➢ Lack of standards inhibits inter-operability ➢ Co-existence of legacy and new technology ➢ No definition of settlement finality	available to investors at certain CSDs, so CSDs have little incentive to adopt ➢ Tokenisation not a solution for assets issued into traditional issuer CSDs ➢ Regulatory driver needed but ill-informed regulators may encourage and possibly inhibit or prevent ➢ National securities laws need to change ➢ Regulatory access must be tempered by respect for privacy	inter-operability standards between national and proprietary distributed ledger networks ➢ Regulatory regimes remain jurisdictional and are liable to clash when distributed ledgers cross borders ➢ Distributed ledgers need to be linked to legacy systems ➢ Management of counterparty identity and KYC checks adds a layer of complexity ➢ All nodes in a distributed ledger network need to own or have access (e.g. via a CSD) to equivalent computing power to sustain transaction volumes and information recovery times or it will create systemic risk ➢ There are potentially lower cost ways of achieving the benefits of distributed ledgers ➢ Regulators will insist banks are responsible to make investors whole even if investors go to issuers direct ➢ Full transparency into beneficial owners already available at certain CSDs ➢ If all nodes in a distributed ledger are subject to a simultaneous cyber-attack, the ledgers will be harder to reconstruct than a single centralized one	inhibiting the sharing of common market infrastructures ➢ Ensure distributed ledgers are in full compliance with all prevailing regulations	between jurisdictions ➢ Some jurisdictions still require proxies to be voted physically ➢ Distributed ledgers would not work in proxy votes without understanding the distinction between legal and beneficial owner of a stock ➢ Likely to be difficult to ensure that the stock register is accurate when the shift is made to a distributed ledger ➢ Double taxation treaties create a need for distributed ledgers to have automatic access to the right information ➢ If distributed ledgers are used in tax reclaims their regulatory status might have to change, especially if they become de facto registers of tax reclaims ➢ Proxy voting is painful, but not painful enough to warrant investment in distributed ledgers since most custodians have outsourced the work anyway ➢ Investor protection and shareholder transparency are not strong drivers for change yet ➢ Banks still required to supply the credit to ensure investors get their dividends on time ➢ In any transition from current systems to distributed ledgers, regulators and tax authorities will need to be part of the design process	which one misstep cascades through the process, while distributed ledgers are simultaneous ➢ More prudent to explore sub-sets of the custody value chain where distributed ledger technologies might be helpful, rather than look to shift the whole chain on to the new technology ➢ Value of corporate actions data processing by custodians might fall to zero in fully functioning distributed ledger environment, which will inhibit adoption