Bulletin

Vol. 81, No. 12

November 2018

RESERVE
BANK
OF NEW ZEALAND
TE PŪTEA MATUA

Reserve Bank of New Zealand *Bulletin*

Subscribe online: https://www.rbnz.govt.nz/email-updates

For back issues visit: https://www.rbnz.govt.nz/research-and-publications/reserve-bank-bulletin

Copyright © 2018 Reserve Bank of New Zealand

ISSN 1177-8644

FinTech developments in banking, insurance and FMIs

Riki Fujii-Rajani

This article is motivated by the recent rapid growth in technology-enabled innovation in financial services, referred to as 'FinTech'. It explains and gives examples of developments in a number of broad categories of FinTech, and considers their implications for the Reserve Bank as prudential regulator. FinTech has the potential to enhance financial sector efficiency, but may also create new risks to financial sector stability. So far the overall impacts have been small, and for now the appropriate response by the Reserve Bank is limited to increased monitoring of emerging FinTech developments.

1 Introduction

'FinTech' (financial technology) is a term with many meanings. For the purposes of this article, FinTech is defined as "technology-enabled innovation in financial services that could result in new business models, applications, processes or products with associated material effect on provision of financial services" (Financial Stability Board, 2017). Such innovations have not been unusual historically, but the pace and scope of change has been particularly striking over recent years.

This article summarises the range of current FinTech innovations and their implications in banking, insurance[1] and financial market infrastructure (FMI), from the perspective of the Reserve Bank of New Zealand (Reserve Bank) as the prudential regulator and supervisor of banks, insurers, and (soon) FMIs[2] in New Zealand. The implications of FinTech for the Reserve Bank's supervisory responsibilities for AML/CFT[3]

[1] The term 'InsurTech' is also used to refer to FinTech arising in the insurance industry.

[2] The Reserve Bank will have increased oversight powers over systemically important FMIs if the current FMI Bill is enacted.

[3] Anti-money laundering and countering the financing of terrorism.

are outside the scope of this article. While the article does not consider non-bank deposit takers (NBDTs) separately, the implications of FinTech for the Reserve Bank's role as the regulator of NBDTs can mostly be inferred from the analysis of how FinTech may affect banks.

This article divides technologies that are generally referred to as FinTech into the following broad categories:

Distributed Ledger Technology (DLT) and blockchain:

- crypto-currencies;
- Application Programming Interfaces (API);
- Big Data and Artificial Intelligence (AI);
- digital platforms encompassing peer-to-peer (P2P) activities; and
- other developments, not included in any of the above.

The following sections 2-7 cover each of these categories in turn, first of all providing a high-level explanation of what the technology is, and then going on to give examples of existing and potential applications of the technology in banking, insurance, and FMIs in turn. Both New Zealand and overseas examples are included.

Each section then draws out some tentative implications for the role of the Reserve Bank, in relation to its mandates to promote financial system stability and efficiency. Under section 68 of the Reserve Bank of New Zealand Act 1989, the Reserve Bank prudentially supervises banks[4] for the purposes of:

- promoting the maintenance of a sound and efficient financial system; or
- avoiding significant damage to the financial system that could result from the failure of a registered bank.

For the purpose of this article, the efficiency part of the mandate is treated as an objective to be considered jointly with soundness. In imposing minimum requirements to help maintain financial system soundness, the Reserve Bank may promote efficiency through:

- modifying or removing requirements that are no longer apt, especially where compliance is costly;
- allowing flexibility in the application of standards where appropriate;
- modifying requirements where appropriate to allow new products into the market, subject to resources and capabilities of the Reserve Bank;
- reducing barriers to entry, provided it does not materially negatively impact soundness; and
- ensuring a level playing field by aligning requirements to the extent possible except where there is a real difference in characteristics that justifies policy variation.

[4] Broadly the same purposes apply to the Reserve Bank's roles in respect of: NBDTs under the Non-bank Deposit Takers Act 2013; FMIs under Part 5B of the RBNZ Act; and insurers under the Insurance (Prudential Supervision) Act 2010.

For convenience, an Appendix summarises and reorganises the material in sections 2-7, to show the impacts for each of the main financial system sectors in turn, rather than by type of FinTech.

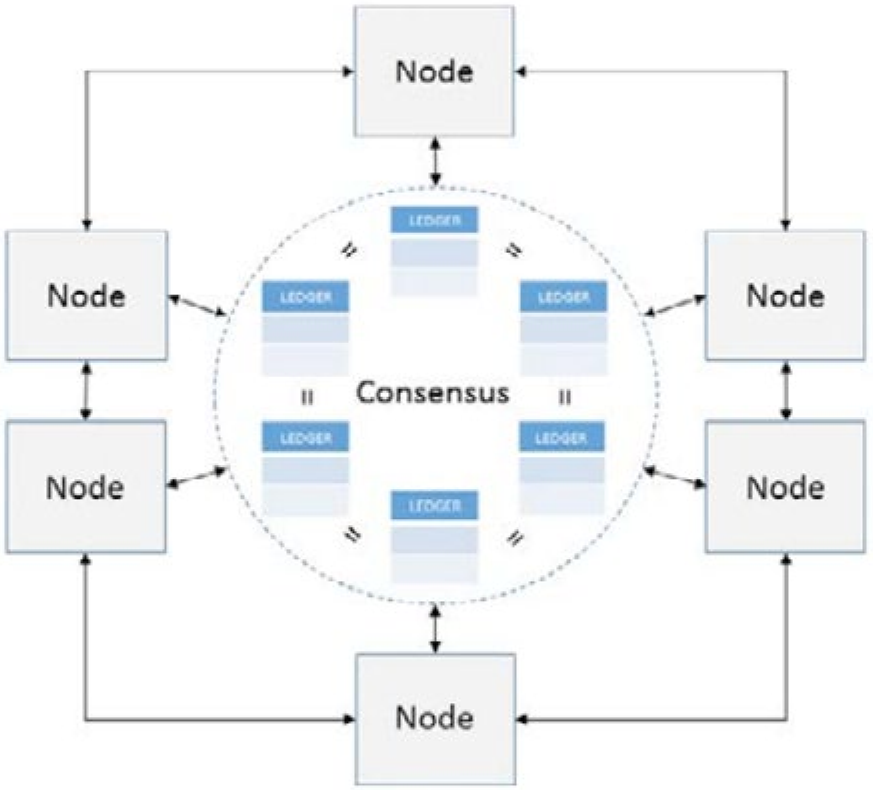
Section 8 considers some ways in which FinTech may affect cyber risks, and the final section draws out some broader conclusions for the future of the financial system and the Reserve Bank's role in it.

2 DLT, blockchain, and smart contracts

DLT refers to the processes and related technologies that enable participating computers (nodes) in a network or arrangement to securely propose, validate and record state changes to a synchronised ledger that is distributed across the network's nodes.[5] A distributed ledger (DL) is a ledger that maintains a history of all transactions, which is shared across a network of multiple sites, geographies, or institutions. This is illustrated in figure 1. DLT has the potential to affect fundamental systems and processes.

Blockchain is a specific instance of DLT with certain characteristics that make it highly resilient to cyber-attacks.[6] Transactions are recorded in batches of 'blocks' and a blockchain is a chain of history of transactions. Blocks must be verified by nodes (referred to as 'miners' in a crypto-currency context) before they are linked to the chain of previous transactions. All participants within the network have an identical copy of the ledger, and all copies of the ledger are updated and maintained cryptographically, through a verification process where verifiers reach a consensus on the changes to the ledger. Figures 2 and 3 illustrate how a blockchain is updated. Note that not all DLs necessarily

Figure 1
Illustration of transactions in a decentralised network

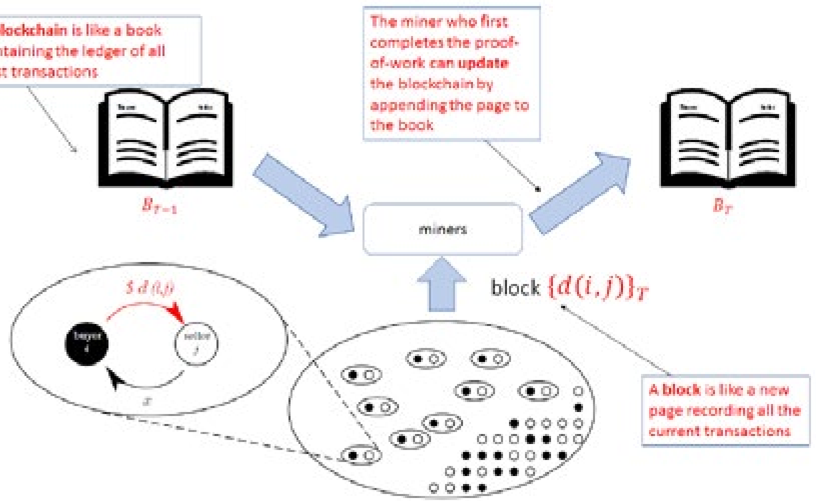


Source: Committee on Payments and Market Infrastructures (2017).

[5] As defined in Committee on Payments and Market Infrastructures (2017).

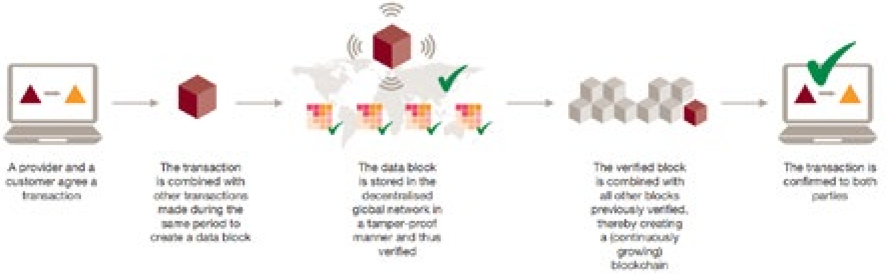
[6] These characteristics are: decentralised, public, independent, open to everyone, borderless, proof-of-work, open source, uncensorable, and immutable (Morgan, 2017).

Figure 2
How a blockchain is updated


A blockchain is like a book containing the ledger of all past transactions
The miner who first completes the proof-of-work can update the blockchain by appending the page to the book
B_{T-1}
miners
B_T
block $\{d(i,j)\}_T$
$ d(i,j)
buyer i
seller j
x
A block is like a new page recording all the current transactions

Source: Chiu and Koeppl (2017)

Figure 3
Alternative illustration of blockchain process


A provider and a customer agree a transaction
The transaction is combined with other transactions made during the same period to create a data block
The data block is stored in the decentralised global network in a tamper-proof manner and thus verified
The verified block is combined with all other blocks previously verified, thereby creating a (continuously growing) blockchain
The transaction is confirmed to both parties

Source: PwC (2016)

employ blockchain technology,[7] and DLT and blockchain should be distinguished.[8]

Consensus is reached through the use of cryptographic tools, and verification contributes to the system's resilience to cyber-attacks. For example, in the context of bitcoins, verification prevents double-spending and creation of false records. The process is as follows (see also figure 4):

- the person seeking to make a change to the ledger creates a transaction message using a private key, and signs it using public key cryptography. This creates a public key that can be used to decrypt the message;

- the person broadcasts the signed message and corresponding public key to the network, for verification;

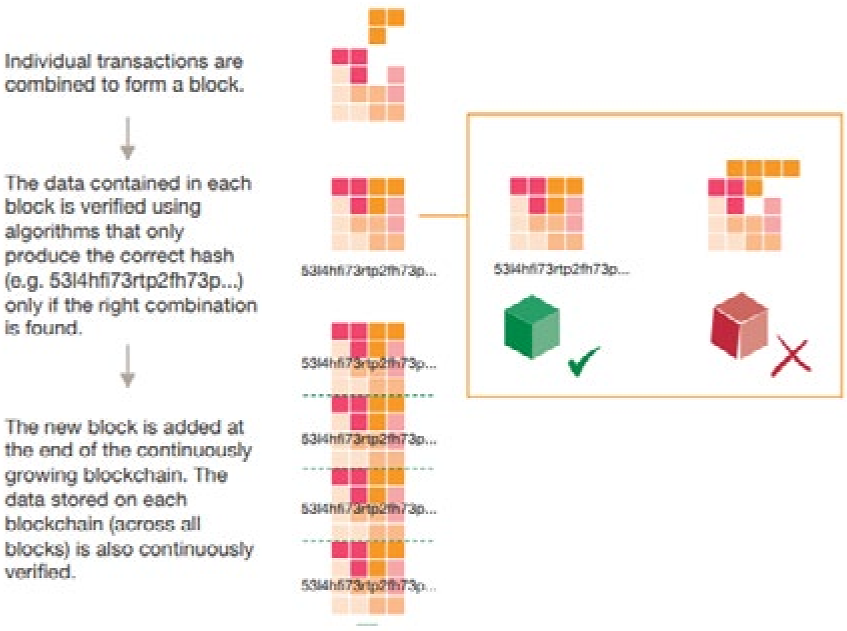
- verifiers ('miners' in the bitcoin context) create candidate blocks using the transaction message, and compete to verify the blocks. Verification of ledger updates can usefully be categorised into two stages:

- authentication: Using a record of previous states, each verifier identifies state changes that are consistent with the rules of the arrangement. This can include, for example, checking digital signatures, availability of assets, sufficiency of funds, and right to transact.

[7] An alternative form of DL may update only users' accounts (Committee on Payments and Market Infrastructures, 2017)

[8] An in-depth description on the mechanics of crypto-currencies and blockchain technology is provided by Kumar and Smith (2017).

Figure 4
Illustration of verification


Individual transactions are combined to form a block.
The data contained in each block is verified using algorithms that only produce the correct hash (e.g. 53l4hfi73rtp2fh73p...) only if the right combination is found.
53l4hfi73rtp2fh73p...
53l4hfi73rtp2fh73p...
The new block is added at the end of the continuously growing blockchain. The data stored on each blockchain (across all blocks) is also continuously verified.
53l4hfi73rtp2fh73p...
53l4hfi73rtp2fh73p...
53l4hfi73rtp2fh73p...
53l4hfi73rtp2fh73p...
53l4hfi73rtp2fh73p...

Source: PwC (2016)

Validation: To add the block to the chain, each verifier undertakes a computational analysis, or in the case of blockchain, 'proof of work'.[9] Proof of work is difficult to achieve, but easy to check. When other nodes accept the update, there is a consensus, and the block is added to the chain.

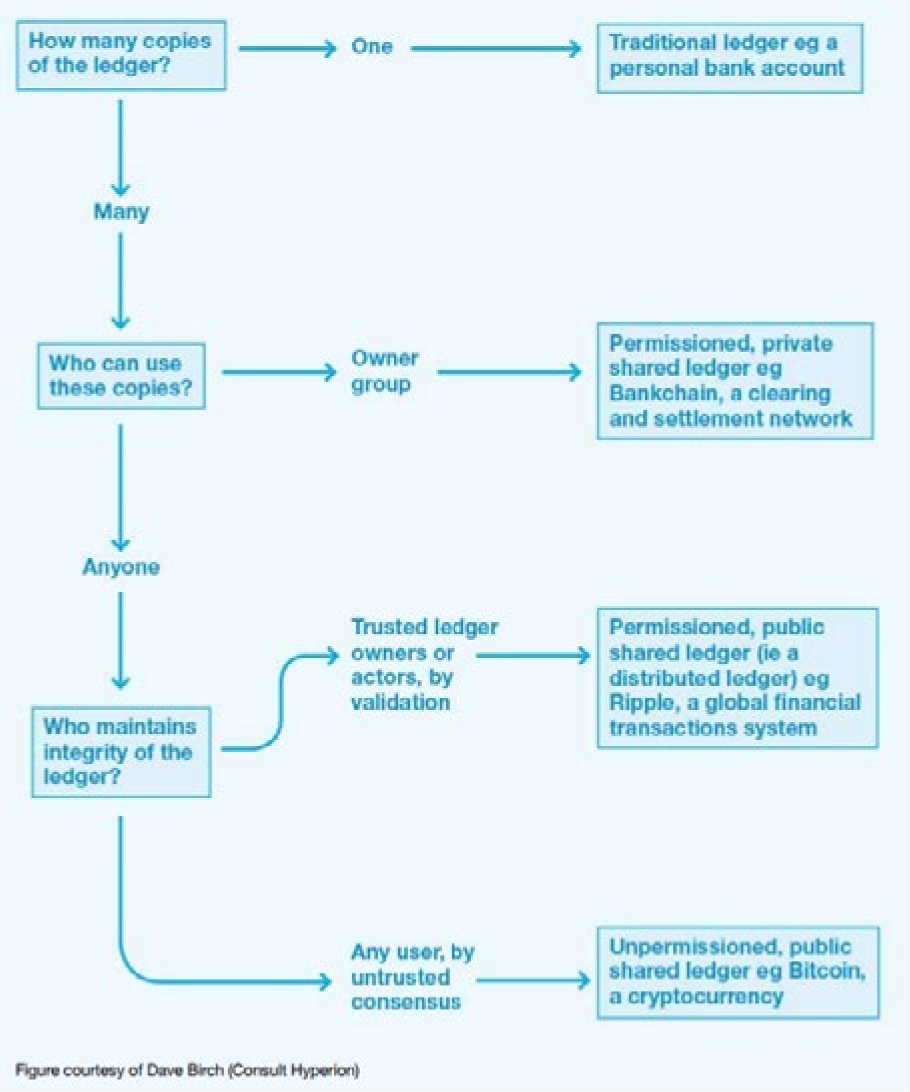
DLs can have various characteristics, depending on how they are designed. For example, a DL can be configured to restrict operations, access, and validation. Blockchain is DLT with a specific set of characteristics. A characteristic of a DL that is useful to understand is whether it is permissioned or unpermissioned. Permissioned ledgers allow only specified individuals or organisations to verify the contents of the ledger. Permissioned ledgers are more efficient, as they do not require a large network of verifiers that can result in duplication of verification efforts and high computational costs.[10] Unpermissioned ledgers are those described above, where anyone can validate transactions. A DL can also be configured to restrict operations, access, and validation. Figure 5 shows one way of categorising different ledger arrangements, to illustrate DLT. Note that blockchain is a form of unpermissioned DLT, but unpermissioned DLT does not equate to blockchain as it depends on what other characteristics are present in the system.

DLT can also be used to record legal information. Smart contracts are an extension of DLT, which allow agreements to be written in code and executed automatically by the network through predetermined rules and inputs. For example, Ethereum's smart contracts are self-enforcing agreements that are executed by multiple participants in the network, including those not party to the contract. This means that any third party can view the exact terms of the contracts, as transactions are verified by participants before it is included in the ledger. Smart contracts are ruled by technical code rather than legal rules, and while enforcement costs might seem lower, the verification process requires computational resources that create costs borne by the network's participants. The legality of a blockchain-based contract is uncertain, and this may require

[9] Further information on the mechanics of 'proof of work' can be found in Kumar and Smith.

[10] Refer to footnote 12 for an illustration of computational cost.

Figure 5
DL taxonomy


How many copies of the ledger?
One
Traditional ledger eg a personal bank account
Many
Who can use these copies?
Owner group
Permissioned, private shared ledger eg Bankchain, a clearing and settlement network
Anyone
Who maintains integrity of the ledger?
Trusted ledger owners or actors, by validation
Permissioned, public shared ledger (ie a distributed ledger) eg Ripple, a global financial transactions system
Any user, by untrusted consensus
Unpermissioned, public shared ledger eg Bitcoin, a cryptocurrency
Figure courtesy of Dave Birch (Consult Hyperion)

Source: UK Government Chief Scientific Advisor (2016)

an administrative step to transform the smart contract into a legal document until blockchain is accepted as a legal document by law.

DLT presents difficulties for regulators as it does not fit the mould of traditional structures. The fact that DLs are maintained by multiple nodes means that there is no single legal entity in control. This raises questions of where legal responsibility for regulatory compliance lies. Another risk arising from the use of DLT is the possibility of system-wide failure occurring through an error in technical code underlying a DL. Furthermore, the irreversibility of transactions exacerbates the consequences of errors in code.

2.1 *DLT: Banking*

The use of DLT in banking has the potential to reduce banks' reconciliation costs. Reconciliation involves banks using systems to track financial transactions and checking those transactions with their counterparts in other banks. Transactions are currently recorded in a centralised ledger that is shared by all participants, which must be integrated with each participant's own systems. DLT has the scope to remove some of the duplication and costs associated with these processes, including paper-based verification, by allowing all banks' systems to be synchronised and updated.

In theory, a distributed ledger can be used by banks as a single, true record that replaces physical documents. In practice, it is likely that the changes required are so pervasive and fundamental that they would require collaboration between competitors, regulators, consumers, technology experts, and the legal community.

Smart contracts could be used to automate the performance of mortgage contracts or trade finance. In 2016, CBA and Wells Fargo in the US completed the first open account transaction using a permissioned DL based on blockchain, where they used a smart contract for cotton shipping from Texas to Qingdao, China.[11] The Hong Kong Monetary Authority (HKMA), alongside Bank of China (Hong Kong), Bank of East Asia, Hang Seng Bank, and HSBC have also completed a proof of concept for DLT and smart contracts in trade finance. The HKMA has indicated that it will continue to explore the possibility of materialising the value from this proof of concept, and noted that legal, regulatory, and governance issues needed to be considered.

JP Morgan, in partnership with Ethereum, has developed a permissioned DLT and smart contract platform, Quorum, for processing private transactions within a group of known participants.

The use of DLT in banking is relevant to the efficiency aspect of the Reserve Bank's responsibilities, as it could eliminate the need for reconciliation of individual ledgers, and smart contracts could automate the performance of contracts. However, the verification process in DLT could involve significant computational costs, as evidenced by the computational resources required for blockchain verification.[12] While the Reserve Bank may facilitate collaboration towards the use of DLT across banks, for example through encouraging investments in common resources, DLT may not be feasible in the near future as implementation of DLT may be hindered by the need for DLT systems and non-DLT legacy systems to interact.

2.2 DLT: Insurance

The use of blockchain in insurance can lower operational costs through reduced duplication of processes, counterparty risks, and increased automation. DLT can facilitate sharing of information to reduce fraud, for example between insurer and hospitals for health insurance, or between insurer and weather experts for crop insurance. DLT can also be used by reinsurers in underwriting reinsurance treaties, by providing a validated contract for version control.

Other DLT applications include automation through smart contracts and managing policies and claims through decentralised autonomous organisations (DAO). DAO is a self-regulated autonomous insurance business model for managing policies and claims, without human employees or control by a single entity, which is implemented by blockchain. Smart insurance contracts could allow automated claims settlement, with claims being paid out without the policyholder filing the claim, or insurer administering the claim. Smart contracts could also be applied to 'parametric loss products'. This refers to a contract that pays out when certain trigger conditions are met, rather than when a loss is incurred. For example, travel insurance could use DLT to trigger a pay-out when a flight management database supplies information that a flight is cancelled.

These uses could lower costs and improve efficiencies, thus reducing non-regulatory barriers to entry for non-traditional companies. Incumbent insurers, on the other hand, may decide to adopt DLT. It could also increase the level of interconnectedness since DLT platforms may need to be standardised across the sector.

While DLT has potential use in insurance sector, it is still in its infancy. Groups of firms are reviewing possible uses of DLT, for example

[11] https://www.commbank.com.au/guidance/newsroom/CBA-Wells-Fargo-blockchain-experiment-201610.html, downloaded 3 October 2018.

[12] The country closest to bitcoin in terms of electricity consumption is currently Austria. If the bitcoin network were a country, its energy consumption would rank above Chile and the Czech Republic. Source: http://digiconomist.net/bitcoin-energy-consumption, downloaded 3 October 2018.

Blockchain Insurance Industry Initiative[13] (B3i) and R3. The focus appears to be on creating immutable insurance claim records, P2P insurance, and more accessible and paperless records of ownership of insured items (asset provenance) to assist risk profiling and claims processing.

For example, Everledger provides provenance confirmation for diamonds, using permissioned and unpermissioned blockchain to track ownership. This is relevant to insurers because upon payment of a claim for a lost diamond, the insurer becomes a rightful owner of the lost diamond. Since diamonds do not generally depreciate in value, it is an asset to the insurer. Being able to track the ownership of the diamond facilitates its recovery and discourages fraud. This use of blockchain is not limited to diamonds, and can be applied to a range of high value goods.[14]

The use of smart contracts in transacting a natural catastrophe swap[15] has been tested by Allianz Risk Transfer and Nephila. The test found that smart contracts accelerated the transactional processing and settlement between insurers and investors, as the smart contract picks up the trigger event from predefined sources and automatically activates pay-outs to contract parties. The test also found that there could be applications in other insurance transactions.[16]

InsurETH is a start-up that uses Ethereum's blockchain platform and smart contracts to offer automated flight insurance. The premium payment is recorded on the Ethereum blockchain, and proof for claims are automatically sourced from public data feed, Oraclise. This allows claims to be paid automatically, without the policyholder being aware of the extent of his or her coverage.

There appears to be no immediate need for a regulatory response to these developments, although they point to some possible areas of focus for the Reserve Bank in future. The Reserve Bank may in due course need to coordinate with industry so that possible efficiency gains can be harnessed in a positive fashion. It may also need to monitor non-traditional companies emerging to take advantage of lower barriers to entry and assess their impact on the stability of the insurance sector, and be alert to a potential increase in liquidity risk from increased claims efficiency. The use of DAO may also raise questions of who is responsible for regulatory compliance.

2.3 DLT: FMI

DLT may be applied to payment, clearing, and settlement processes to decrease end-to-end transaction times and enhance efficiency, transparency, and resilience. DLT would allow maintenance and agreement of mutual information without additional reconciliation, while decentralised verification by a number of participants strengthens the system against corruption. Replication of information to participants in real time enhances transparency and improves system resilience by reducing the risk of a single failure affecting the data.

The extent of these benefits depends on the arrangement. For example, the Blockchain form of DLT could allow new entrants and reduce tiering

[13] B3i firms include Swiss Re, Munich Re, Zurich, Aegon, Hannover Re, Generali, Ageas, Liberty Mutual, Achmea, RGA, SCOR, Sompo Japan Nipponkoa Insurance, Tokio Marine, XL Catlin, and Allianz.

[14] https://www.everledger.io/

[15] A catastrophe swap is a financial instrument which transfers a specific set of risks, usually those of natural disasters, from an insurer to investors or other insurers. A financial catastrophe swap involves the insurer paying a third party to assume the financial risk of a defined catastrophe event, in exchange for a payment. If the event occurs and meets the pre-determined trigger criteria, the third party is responsible for the pre-agreed financial risk.

[16] http://www.agcs.allianz.com/about-us/news/blockchain-technology-successfully-piloted-by-allianz-risk-transfer-and-nephila-for-catastrophe-swap-/, downloaded 3 October 2018.

of relationships[17] by removing the need to have records of individuals' accounts stored centrally at a bank, or the need for banks' reserve accounts to be held centrally at the central bank. On the other hand, the unpermissioned nature of Blockchain may create scalability issues: bitcoin blockchain for example is limited to processing four to seven transactions per second with each block taking around 10 minutes to mine,[18] compared to Visa which processes 2,000 transactions per second. However, the limit on bitcoin's transaction volume is due to protocols that limit the size of transaction blocks to 1 mb, and that adjust the difficulty of computational problems to ensure that processing time is kept constant at around 10 minutes. While this design is intended to enhance blockchain's resilience, note that the 'forking' of Bitcoin and Bitcoin Cash in August 2017 was motivated by a difference in opinions about how to make transaction processing more efficient.[19] Another issue may be information security problems because of the public nature of blockchain: anyone can see transactions, and verifiers are anonymous.

A DL that did not have the permissionless feature of Blockchain would allow consensus to be achieved more quickly. But it might also be less resilient: having fewer nodes verifying transactions means that one compromised node can have a greater impact on the integrity of the ledger. Having fewer nodes also results in a similar system to the existing system of trusted central counterparty. A key risk in DLT generally is a lack of settlement finality and legal uncertainty. Ledgers are updated on a majority vote, and unlike traditional certainty of legally defined finality, settlement is therefore probabilistic with transactions merely less likely to be reversed as more participants consider the transaction as settled. This leads to legal uncertainty, but also it is unlikely for a block to be reversed once other blocks are added to the chain.

In New Zealand, the Reserve Bank provides ESAS as a real time gross settlement (RTGS) system. DLT is not being considered by the Reserve Bank in its ESAS technology replacement project.

Central banks of Canada, the UK, Japan, Europe and Singapore have begun experiments to study the viability of DLT in wholesale payments, with a focus on RTGS systems.[20] No central bank has implemented a major DLT solution outside experimental conditions. In a report published in June 2017, the Bank of Canada concluded that DLT in its present state may not provide overall net benefit in comparison to current centralised systems (Bank of Canada 2017).

The Bank of England has indicated that its next generation RTGS service will be compatible with settlement in a DL. The Bank of England's FinTech Accelerator has worked with Ripple[21] in a proof of concept to determine whether the Interledger Protocol[22] ('ILP') can be applied in its RTGS. The proof of concept found that the ILP protocol was able to synchronise payments between two simulated RTGS ledgers, with the ILP Validator creating a single source of truth. It also found that cross-border payments in wholesale markets had different challenges to retail and corporate transactions, for example the availability of liquidity. The Bank of England and Ripple will begin to explore these questions, and

[17] Indirect access to an FMI can be efficient for smaller users, but excessive tiering may create concentration risks. See section 6.3 below.

[18] http://www.ibtimes.com/bitcoins-big-problem-transaction-delays-renew-blockchain-debate-2330143, downloaded 3 October 2018.

[19] For a non-technical explanation of the split, refer to http://theconversation.com/bitcoin-splits-and-bitcoin-cash-is-created-explaining-why-and-what-happens-now-81943, downloaded 3 October 2018.

[20] See Watson (2018a) for a further discussion of the role of DLT in payments processes generally, and an analysis of the Canadian and Singaporean experiments in particular.

[21] Ripple is a crypto-currency that has been established specifically to make cross-border bank-to-bank transactions easier.

[22] The Interledger Protocol ('ILP') is not centralised or decentralised, but relies instead on the use of escrowed transfers (conditionally locked transfers). The ILP connects disparate ledgers and a subledger (the ILP Ledger) that temporarily puts funds on hold across all parties. The ILP Validator then cryptographically validates the hold, and signals all parties to release funds simultaneously

the Bank of England is considering further proofs of concept.[23] The Bank of England is also a member of Hyperledger, an open source collaborative effort that aims to advance cross-industry blockchain technologies.

R3, a blockchain consortium, has completed a DL experiment involving 11 of its member banks[24] being connected in a private peer-to-peer DL, and has released Corda. Corda[25] is a DL platform for recording and processing financial agreements, and supports smart contracts. It is designed for regulated financial institutions, and enables participants to transact without the need for central authorities. More than 40 banks from more than 15 countries, including Westpac, Commonwealth Bank of Australia, and HSBC, have invested in the platform.

In Australia, the Australian Securities Exchange (ASX) is currently developing a replacement for CHESS (Clearing House Electronic Subregister System), based on permissioned DLT[26]. The Sydney Stock Exchange is also working towards a blockchain-based settlement platform.[27]

SWIFT is undertaking a blockchain proof of concept with 22 global banks, including Westpac (Australia), with ANZ (Australia) taking part as a founding member. SWIFT is exploring the potential use of blockchain technology in helping banks reconcile their international nostro accounts in real time, through a permissioned DL with a closed user group. This forms the third phase of 'SWIFT global payments innovation', to which more than 110 banks have signed up, including banks with New Zealand subsidiaries.[28]

CLS is developing a standardised, automated payment netting service, CLSNet, for FX trading settling outside the CLS settlement service, with participants being able to submit FX instructions through traditional SWIFT channels or DLT.

SETL, a start-up based in the UK, has partnered with Cobalt DL[29] to launch OpenCSD within Cobalt's FX platform. OpenCSD is a blockchain-based platform that creates a single, shared view of each FX transaction. It enables any market participant to commission and run a permissioned registry service for payments, settlement and clearing of cash and other financial settlements.

Potential applications of DLT can enhance FMI efficiency by speeding up transactions and reducing settlement time by eliminating the need for additional reconciliation. This would reduce the amount of time each counterparty is exposed to another, and free up collateral and capital for other productive uses. However, the UK Financial Conduct Authority (FCA) has noted that many of the benefits of DLT, such as faster settlement, may be achievable through traditional technology. The fact that this has not been achieved may be due to market preference, rather than technological constraint. Another reason may be the need for investments into shared technology, which creates an externality problem of underinvestment and free-riding.

[23] https://www.bankofengland.co.uk/news/2017/july/fintech-accelerator-results-of-latest-round-of-pocs, downloaded 5 October 2018.

[24] Barclays, BMO Financial Group, Credit Suisse, Commonwealth Bank of Australia, HSBC, Natixis, Royal Bank of Scotland, TD Bank, UBS, UniCredit and Wells Fargo.

[25] https://docs.corda.net/_static/corda-introductory-whitepaper.pdf

[26] https://www.asx.com.au/documents/asx-news/ASX-Selects-DLT-to-Replace-CHESS-Media-Release-7December2017.pdf

[27] https://www.coindesk.com/sydney-stock-exchange-blockchain-prototype/, downloaded 5 October 2018

[28] ANZ (Australia),Bank of Tokyo-Mitsubishi, Bank of China, China Construction Bank, Citibank, Commonwealth Bank of Australia, HSBC, ICBC, JPMorgan Chase Bank, National Australia Bank, Rabobank, and Westpac Banking Corporation https://www.swift.com/news-events/press-releases/22-additional-global-banks-join-the-swift-gpi-blockchain-proof-of-concept

[29] Cobalt DL is a peer-to-peer network that reduces post-trade cost and risk for financial market participants through DLT.

Blockchain DLT could alleviate systemic operational risk by reducing the financial system's reliance on a centralised third party, and by having a number of contributors maintaining back-ups. It could also be more resilient to cyber-attacks, as the attack must affect all copies of the DL simultaneously. While DLT tends to be resistant to unauthorised change, it is not invulnerable to cyber-attacks, as anyone who can find a way to legitimately modify one copy of the ledger can modify all copies of the ledger.

Theoretically, bitcoin blockchain is vulnerable if more than 50 percent of computer processing power for bitcoin is controlled by a single individual or organisation, but it is not vulnerable to a cyber-attack on a particular user. Blockchain has been secure against cyber-attacks thus far, due to the difficulty of controlling more than 50 percent of computing power. However, the same conclusion cannot be drawn for DLT, as DLT may not necessarily have the same characteristics as blockchain. For example, permissioned DLT can render the system vulnerable to a cyber-attack on a particular user.

Under the proposed new FMI oversight framework in New Zealand[30], the definition of FMI is worded openly to allow FMIs based on non-traditional technologies to be covered under the definition. It is proposed that the Reserve Bank will have information-gathering powers over all FMIs (including new entrants to the financial system), and enhanced oversight powers over systemically important FMIs, including the power to set prudential standards around risk management, systems and controls. If a new FMI based on DLT emerges, it would likely be non-systemic and not subject to standards set by the Reserve Bank in its early stages. So the proposed framework would promote efficiency by reducing barriers to entry for new, innovative FMIs. However, if an FMI based on DLT subsequently grew to become systemic, it would become subject to prudential standards. This may help address the risk of general business losses impairing provision of critical services, for example if the operators of a new FMI specialise in other business lines such as technology or data aggregation. The Reserve Bank may need to ensure that the standards it imposes on FMIs are adequate to cover risks specific to DLT, which may differ to those of traditional systems. Looking further ahead, it may become necessary to impose prudential standards tailored for non-traditional technologies, such as DLT.

3 Crypto-currency

'Digital currency' refers to any currency that represents value electronically[31]. It may be denominated in legal tender: for example, in modern financial systems, a transaction account held at a bank is typically a form of digital currency. A crypto-currency is a decentralised currency that is transacted using DLT and uses cryptography to secure transactions and validate balances. Bitcoin is a specific example of a crypto-currency based on blockchain technology.

An extension of bitcoin technology is 'coloured coins'. A coloured coin is a basic bitcoin with additional attributes or restrictions programmed into it, so that it carries more than mere value. Examples of attributes or restrictions include purpose of use, expiry date, and location of use. Coloured coins can be programmed so that failure to pay on time or

[30] Legislation establishing the framework is currently being drafted.

[31] For a fuller discussion of digital currency in the context of different forms of money, see Wadsworth (2018).

expiry of contract results in revocation of the electronic access key. This can be used for smart contracts and securities transfers.

Although the relationship between a bitcoin wallet and its owner(s) is obscured, the chain of transactions in and out of the wallet is visible to the public. There has been some development of methods to strengthen the privacy of transactions, for example through mixing bitcoins from multiple users so that the output coins are not linked to the original users. However, this merely hides the user within a limited list of potential users, and there are statistical methods to de-anonymise the transactions.

An issue with some designs of crypto-currency is the speed with which transactions can be processed. For example, bitcoin transactions must be assembled into blocks of one megabyte before verification. This means that about only seven transactions can be processed per second, in comparison to the thousands of transactions that can be processed by conventional payment systems.

3.1 Crypto-currency: Banking

Crypto-currencies that are similar to Bitcoin allow payments directly between payer and payee without intermediaries such as commercial banks. Banks could become involved by working with start-up companies to develop trusted crypto-currencies, or crypto-currencies may be used for lending activities.

New Zealand banks do not appear to be getting involved with existing types of crypto-currency at this stage. On the contrary, banks have been reported to close down accounts associated with bitcoin operations, apparently because of concerns about them being used for money-laundering. For example, Bitnz, a New Zealand bitcoin exchange platform, attributed its closure to the refusal of New Zealand banks to allow bank accounts for the purpose of trading bitcoins.[32]

LHV Bank in Estonia[33] became the first bank in the world to experiment with programmable money (also called 'coloured coins'), by issuing Cryptographic Universal Blockchain Entered Receivables (CUBERs) each worth 100,000 euros. CUBER is a new type of certificate of deposit, which is cryptographically protected by being recorded in a bitcoin blockchain. Acquiring CUBERs means acquiring a claim against LHV Bank, of a value equal to the value of the CUBERs. The CUBER app is a smartphone application that acts as an electronic wallet. It allows the use of CUBERs for payment to other CUBER app users. This allows instant and free peer-to-peer euro transactions, as well as low-cost electronic payments for purchase of goods and services from merchants using the CUBER app. There is no need for CUBER app users to know that it uses bitcoins, as bitcoins are merely used as a data carrier and represents a claim in fiat currency against LHV Bank. CUBER can be acquired from LHV Bank or from other users. CUBER trading occurs without any third party intervention, and a customer relationship with LHV Bank is only required if CUBERs are acquired from, or redeemed by, the LHV Bank.[34]

CUBER can be used to store, generate, and transfer value, as well as managing liquidity and automating transactions. As CUBER's code and API are open source and available to third parties online, it is theoretically possible for New Zealand banks or NBDTs to import the technology.

Commercial banks may facilitate access to privately issued crypto-currencies. Norway's largest online-only bank, Skandiabanken,

[32] https://news.bitcoin.com/new-zealand-exchange-bitnz-shuts-down-banking-hostility/, downloaded 3 October 2018.

[33] Also known as AS LHV Pank.

[34] http://www.cuber.ee/en_US/, downloaded 3 October 2018.

announced plans to offer clients the ability to link bank accounts to their crypto-currency holdings in Coinbase, to allow users to view their crypto-currency holdings within the bank's app. In New Zealand, MyBitcoinSaver offers the world's first dedicated bitcoin savings platform to enable users to invest in bitcoins by setting up automatic payments to be 'saved' in bitcoins.[35]

Crypto-currencies can also be used in lending activities outside banks. An example is ETHLend, a P2P lending platform for Ether,[36] where users can borrow Ether through a smart contract. Loans can be secured with collateral in the form of collateral tokens[37] or Ethereum Name Service Domains, which are transferred to the lender upon the borrower's failure to pay. A borrower earns 0.1 Credit Tokens for each Ether that is repaid, and the borrower is entitled to access unsecured loans of an amount equal to the Credit Tokens he or she possesses. If the borrower fails to repay a loan (secured or unsecured), all of the borrower's Credit Tokens are permanently deleted. The lending activities are decentralised, and loans are made directly between the borrower and the lender without intermediaries. ETHLend does not hold assets and has no power to stop lending activities of its users.[38] There are also P2P lending platforms for bitcoins, although one such platform, BTCJam, cited "regulatory challenges" and "difficulties faced in introducing bitcoin technology to poor communities" as reasons for closing its operations.

Another use of crypto-currency in lending activities is the use of crypto-currency to secure cash loans in national currencies. For example, SALT Lending in the US matches borrowers to lenders based on the value of the borrower's crypto-currency asset, such as bitcoins, rather than their credit scores. SALT keeps the collateral assets in its architecture during the loan period. Loans are originated by a SEC registered investment advisor, and SALT is a non-bank entity that is subject to supervision by state agencies responsible for monitoring consumer credit, trade, and commerce, as well as the Consumer Financial Protection Bureau, and the Federal Trade Commission.[39]

Fisco, a Japanese financial information firm, has announced that it is experimenting with a bitcoin bond. The bond was released for an internal trial in August 2017, with a 3 percent annual interest rate over three years and a return in bitcoins upon maturity. Chicago Board Options Exchange launched trading in bitcoin futures contracts in December 2017.[40]

At the time of writing this article, crypto-currencies are not widely used and the main activity involving them amounts to the mere buying and selling of them as a commodity. The more wide-spread adoption of crypto-currencies, for example their use in lending, might have systemic implications for liquidity and funding. For the time being, it is appropriate for the Reserve Bank to keep monitoring developments in this area and to engage with industry stakeholders as appropriate.

[35] See https://mybitcoinsaver.com/about. This is not a deposit-taking activity under the Reserve Bank's jurisdiction, as it is more analogous to a non-discretionary investment scheme.

[36] Ether is described as a 'crypto-fuel' for operating the distributed application platform Ethereum. It is different from bitcoins in that it is not intended to be used as a currency, but rather, as a token to pay for computation.

[37] A collateral token can be any ERC20 Token, which is a token that conforms to Ethereum's token standard.

[38] https://ethlend.io/en/, downloaded 3 October 2018.

[39] https://saltlending.zendesk.com/hc/en-us/sections/115002565167-The-Company, downloaded 3 October 2018.

[40] http://cfe.cboe.com/cfe-products/xbt-cboe-bitcoin-futures, downloaded 3 October 2018.

3.2 Crypto-currency: Insurance

Digital currencies do not appear to have significant implications for the insurance industry. Crypto-currencies may be used in conjunction with a P2P platform or used in DLT-based insurance. For example, InsurETH (referred to in Section 2.2 above) denominates its payments in pound sterling but uses Ether, the cryptocurrency of Ethereum, in making payments and the policyholder is required to create an Ether wallet.

These crypto-currency uses do not have significant implications for the Reserve Bank's financial stability or efficiency mandate.

3.3 Crypto-currency: FMI

A possible application of cryptocurrencies is in the field of cross-border transactions/remittances. Cross-border transfers under existing mechanisms are costly and slow, as they must be processed through intermediaries and can pass through a number of banks before reaching their destination. As a result, settlement can take up to five days for most common currency pairings. The IMF (2017) has identified two possible applications of DLT-based payment mechanisms to cross-border transfers: a privately run hub-and-spoke payments network, and a central bank-issued digital currency.

A privately run hub-and-spoke payments network involves an exchange of fiat currency into cryptocurrency through ATM machines, point of sale terminals, or online interfaces (the 'spokes'). The cryptocurrency, in the form of tokens, is transferred over the currency's secure network (the 'hub') to the recipient's digital wallet. The currency is then converted into foreign fiat currency through the 'spokes'. This allows transfers of small amounts at lower cost, executed in a shorter timeframe, while encouraging competition in cross-border transfers. However, there are risks arising from price fluctuation in cryptocurrencies.

The IMF study envisages a central bank digital currency (CBDC) not as a parallel currency, but as a widely-available DLT-based representation of the national fiat money. The concept would introduce a new means of payment and store of value, but not a new unit of account. As the IMF acknowledges, the balance of benefits and costs of introducing a CBDC needs further study.[41]

While there are a number of digital wallets and mobile payment systems, the underlying transactions are ultimately processed through established infrastructures using legacy systems. However, if the payments stay in the form of crypto-currencies, their widespread adoption, for example in cross-border transactions, would reduce the existing role of FMIs such as ESAS. But new payments mechanisms are likely to involve new forms of FMI carrying out new roles.

4 Application Programming Interface ('API')

An API is a set of functions and procedures that allow the creation of application(s) which access the features or data of an operating system, application, or other service. In other words, they are like a contract that

[41] For the Reserve Bank's investigation of this question, see Watson (2018b).

governs how one system can talk to another, even if they have different software or languages.[42]

APIs' ability to allow different systems to communicate has the potential to facilitate regulator-bank interactions and compliance with regulatory reporting requirements in all three sectors. They can also be used to create aggregators, platforms that brings information from different sources together to allow customers to compare prices and switch providers easily.

4.1 API: Banking

In the banking context, APIs can be used to access information contained in a bank's core system. Firstly, this could be used in the process of replacing the core bank systems, where APIs are used to control the communications between front-end and back-end systems, allowing developers to test new back-end software without disrupting front-end systems. Secondly, APIs could be used to allow banks to cooperate with third party developers or start-ups to allow them to create customer-facing applications, through access to information held by the bank. 'Open banking' refers to a standardised and secure framework for sharing bank customer data with other banks and with third parties. This enables third parties to offer a wide range of financial services, such as retail payment mechanisms, automated financial advice, and easy ways to access and manage deposit accounts and bank loans across multiple banks.

In New Zealand, Payments NZ is currently trialling APIs with banks and third parties that will enable accredited third parties to make retail payments on behalf of their customers. The trial, expected to be completed late this year, will help Payments NZ to establish common standards that banks and providers can use to share customer data.[43]

The European Commission issued the Payment Services Directive 2 (PSD2) in January 2016. PSD2 gave member states two years to introduce laws that require banks to give third parties access to their customers' bank account data, conditional on regulator and customer authorisation. It gives customers the right to use Payment Initiation Service Providers and Account Information Service Providers, where the payment account is accessible online and where they have given their explicit consent. While PSD2 does not specify the use of APIs, it is believed that it would enable small businesses to share their banking data with trusted, non-bank third parties via APIs.

In response, the UK Competition and Markets Authority (CMA) formed a group to create the Open Banking Standard, a common set of specifications that banks must follow, addressing the technical rules and security aspects of data-sharing via APIs. The nine largest UK banks were required to publish write-access APIs in line with the standards by February 2018.[44] Third parties will be required to register with the Open Banking Directory of Participants and meet the security requirements outlined in the standards, to provide payment services to the public. The FCA will regulate those registered.

In Australia, the Government published an independent review into open banking in February 2018. It makes 50 recommendations. It proposes that open banking be a multi-regulator initiative, led by the Australian Competition and Consumer Commission, but involving the RBA, APRA,

[42] For further information on APIs, refer to Watson (2016).

[43] For more information, see https://www.paymentsnz.co.nz/about-us/payments-direction/api-framework/, downloaded 3 October 2018.

[44] https://www.openbanking.org.uk/about/

ASIC and Office of the Australian Information Commission. A Data Standards Body should be formed to establish open banking standards, and only accredited parties should be able to receive open banking data. Those parties should be able to receive all customer-provided information and transaction information through an API and free of charge. The review proposes that the industry be given 12 months to implement the proposals following the final government decision, and that it should apply to all banks.

To the extent that banks are initiating collaboration with developers and start-ups using APIs to create customer-facing apps, there would be little need to change the Reserve Bank's supervision of the sector. However, if open banking becomes widely adopted, it could have implications for the sharing of personal data, and for competition. This would primarily be of concern to government agencies such as the Ministry of Business, Innovation and Employment (MBIE), the Commerce Commission (the New Zealand equivalent of UK's CMA) and the Ministry of Justice. But the Reserve Bank is also monitoring the development of open banking as it has the potential to affect the soundness and efficiency of the financial system.

Open banking has the potential to improve the efficiency of the financial system by increasing competition in the provision of financial services. This should help drive down the cost of these services and encourage continued financial service innovation. Greater sharing of customer data could also help financial services to be better tailored to customer requirements, improving the efficiency with which the banking sectors resources are allocated.

Open banking may also have implications for financial stability if it creates more customer churn resulting in weaker, more arms-length client relationships. The loss of customer loyalty may make deposits a less stable source of funding. This increases liquidity risk, while weaker customer ties could reduce the ability to cross-sell and diminish profitability, and could have implications for incumbents' ability to manage credit risk. While the system as a whole is not necessarily weakened, prudential standards may need to be adjusted, for example to treat deposits as less sticky to take weaker customer loyalty into account, or to tighten requirements on banks' estimation of credit risk and monitoring of provisioning.

Although there are no plans to do so currently, the Reserve Bank could, in theory, use APIs in its processes as a supervisor and regulator. This type of technology is referred to as RegTech, which describes the use of FinTech in the regulatory field. For example, APIs could be used to access banks' information as needed, without the need for private reporting. The Banking Supervision Handbook may also be made more accessible.

4.2 API: Insurance

Insurers can provide APIs to draw on data provided by the functions of wearable or other devices, such as cameras, microphones, GPS locators, and time functions. These can be used, for example, to take a picture of damage, identify the location, and time stamp the information. APIs could also facilitate comparison apps if information about the insurer's products are made available through APIs.

Examples of APIs currently offered in the insurance industry include APIs designed to:[45]

- reformat data to avoid manual rekeying of data;
- allow an insurer to retrieve the claims history of a driver and their policies, using the driver's licence;
- develop a rate plan reflecting the risk levels of prospective customers; and
- automate the filing of standard reporting documentation for regulatory compliance.

While APIs can be used to enhance efficiency in the insurance sector, there appears to be little cause for the Reserve Bank to respond.

4.3 API: FMI

APIs can be used in payment systems to enhance interoperability, to act as a 'glue' holding the payments architecture together. The New Payments Architecture that is currently being consulted on in the UK proposes to use APIs, including Open Banking APIs. Proposed uses of APIs include acting as channels to provide access to increased amounts of remittance information for each payment, which provides context on the underlying commercial transaction.

In New Zealand, Payments NZ's Payments Direction programme is currently investigating the feasibility of a shared API network with industry representatives. The programme seeks to improve the efficiency of the retail payments system.

In India, the Reserve Bank of India supports a payments infrastructure based on a set of open APIs, called the Unified Payments Interface. The Interface allows phone-to-phone transfers directly from bank accounts and enables mobile phones to be access points for P2P transfers, remittances, and payments. It also stores transactional history that facilitates credit worthiness assessment.

Transpay's Mass Pay API uses end-to-end single-point API connection to enable businesses to send unlimited mass pay-outs across Transpay's network, including cross-border payments. The funds are sent straight to the recipient's bank account or a preferred cash pick-up location without crossing any intermediary or correspondent bank networks.

5 Big Data and Artificial Intelligence ('AI')

AI involves the use of advanced algorithms to derive patterns from vast data. It can be used to predict behaviour, prices, and make automated decisions mimicking human judgement. Machine learning is an application of AI that gives systems an ability to automatically learn and improve from experience without being explicitly programmed.[46] Deep learning is a subset of machine learning. It can be used for unstructured data, such as text and images, due to a layered method of calculation that starts from high-level abstraction before moving to more specific features.

[45] https://developer.ibm.com/apiconnect/2014/09/12/apis-for-the-insurance-industry/, downloaded on 3 October 2018.

[46] http://www.expertsystem.com/machine-learning-definition/, downloaded 5 October 2018.

Machine learning can improve the efficiency of decision-making processes, and data analytics may facilitate regulatory compliance, by allowing internal data to be converted into regulatory reporting formats.

However, the use of algorithms in interpreting Big Data presents a difficulty for regulators as they are inherently difficult to interpret, and may not be subject to the same governance and auditability standards as banking and insurance models. Therefore the use of AI may require development of monitoring and auditing standards for algorithms in AI.

Big Data is facilitated by cloud computing, which provides scalable on-demand processing and storage for data. Data storage is regulated by the laws and regulations in the country where the storage is located.[47]

'Robo-advice' refers to automated personalised advice services delivered digitally, commonly using AI. It can be used in providing services such as financial recommendations[48], investment or contract brokering, portfolio management, and potentially insurance advice. In New Zealand, the Financial Advisers Act 2008 ('FA Act') requires that financial advisers be natural persons, but the new financial advice regime that is planned to replace the FA Act in 2019 is intended to be 'technology neutral', that is, not to distinguish between natural persons and digital advice services (provided that the required minimum standards of conduct for giving advice are met). As an interim measure, the FMA has issued an exemption from the FA Act, allowing the use of robo-advice for financial advice, including in relation to insurance.[49] The exemption is available to any provider that meets specified conditions, and applies for, and is approved for, the exemption.

While the use of robo-advice in trading and investment falls within FMA's jurisdiction, the FMA's main objective is to "facilitate the development of fair, efficient, and transparent financial markets",[50] and there may be scope for a Reserve Bank response where widespread use of robo-advice may threaten the stability of the financial system as a whole. Risks to financial stability include errors or disruptions in algorithms which are similar across robo-advisors with significant market share, leading to systemic implications, as well as herding behaviour.

Big Data can also be relevant to the Reserve Bank in identifying trends in systemic risk and economic trends more generally. The Bank of England is investigating ways to expand the use of Big Data by making data, for example regulatory mortgage contract data, anonymous to allow wider sharing with external researchers without breaching privacy laws.

Despite the potential of Big Data and AI, it should be noted that there are significant privacy, data protection, and consumer protection concerns that may hamper the implementation of these technologies.

5.1 Big Data and AI: Banking

Big Data and AI can be used in banking to automate credit decisions. They can also support regulatory compliance, customer support, and legal work.

In China, the use of algorithms in transaction and search data to improve credit scoring by e-commerce platforms has resulted in a significant

[47] For example, if a bank stores its customer data in the US, it would be subject to US laws and regulations, such as the USA PATRIOT Act.

[48] Robo-advice for investment involves customers answering a number of questions about their finances, and receiving automated advice on matters such as how much money to invest and types of funds. The robo-advisor can transact on the customer's behalf in return for a fee.

[49] https://fma.govt.nz/compliance/consultation/consultation-papers/consultation-paper-proposed-exemption-to-facilitate-personalised-robo-advice/

[50] Financial Markets Authority Act 2011, section 8.

expansion of credit availability and low default rates. For example, Ant Financial has been authorised to give alternative credit scores, and has reported default rates below 2 percent despite a lack of guarantee or collateral for its micro-loans. Credit scores can also be calculated from non-traditional variables, such as social networks.

AI has also been used by Royal Bank of Scotland and NatWest in chatbots[51] to answer customer queries. Sweden's Swedbank has chatbots that take part in an average of 30,000 conversations per month and can handle more than 350 different customer questions.

JPMorgan has begun using Contract Intelligence (COIN) to automate the interpretation and review of commercial loan agreements. The software reportedly allows tasks that used to take lawyers and loan officers 360,000 hours, to be completed in seconds.[52]

The use of AI to automate processes supports the Reserve Bank's mandate of efficiency, but may have implications for financial stability if it creates difficulties in supervision of banks. For example, the use of AI in credit decisions may require the Reserve Bank to inquire into the algorithms used in a similar manner to internal models, and demand Reserve Bank resources to do so. The nature of the technology also requires specialised knowledge and standards.

In terms of RegTech, the Reserve Bank may use AI to enforce regulatory compliance. The FCA is looking into making its handbook machine-readable and machine-executable, to enable machines to interpret and implement the rules directly. In its call for input, the FCA referred to a 'Robo-Handbook', which would allow firms to interact with the FCA Handbook to understand its impact on their systems and processes, and assist with compliance. It is also investigating speech-to-text software, social media and media analytics, as well as financial processing tools to automate processes.

5.2 Big Data and AI: Insurance

Big Data can be used in product offerings, risk selection, pricing, cross selling, claims prediction, and fraud detection. For example, telematics[53] boxes in cars can monitor driving behaviour to use the data for offering individualised policies and prices, including usage-based insurance. Data may also be sourced from a third party, for example from the public sector.[54] 'Internet of Things' (IoT) refers to the use of sensors in everyday objects, such as machines or wearable devices, to gather data. It can provide information about individuals' behaviours to assist in underwriting and claims stages.

Machine learning and AI can enable the use of data in real time and predict events such as vehicle thefts, health problems, and weather events, to allow better pricing of risks as well as preventive counselling. This can be used in the underwriting process and allows new types or tailored products to be offered. For example, AI can be used to analyse photos to determine medical conditions, such as skin cancer. Underwriting life insurance can be facilitated by a calculation of the individual's life expectancy through the use of facial recognition technology for predicting factors such as age, gender, smoking habits,

[51] A chatbot is a computer program that conducts a conversation.

[52] https://www.bloomberg.com/news/articles/2017-02-28/jpmorgan-marshals-an-army-of-developers-to-automate-high-finance, downloaded 3 October 2018.

[53] Telematics is a branch of technology which deals with the long-distance transmission of computerised information, for example GPS systems.

[54] The UK, US, and the European Union have launched 'open data' websites to make available government statistics, including health, education, worker-safety, and energy data.

and BMI, used in conjunction with an activity sensor such as a FitBit or physical activity tracker on a mobile phone.

Robo-advice can be used to collect client information to understand needs and preferences, and to propose, implement, and maintain the policy. This removes or reduces the involvement of a human advisor. While robo-advice is more prevalent in the investment advisory sphere, there is some extension into the insurance sector by firms that provide both insurance and investment advice. For example, the Royal Bank of Scotland has announced that it would be introducing robo-advisers to replace staff, including those who had provided advice on insurance products.

An example of AI in use is Lemonade's AI app designed to make an offer of an insurance policy. The AI app takes into account risk mitigation factors such as sensitivity of homes to severe weather events and discounts for protection equipment such as fire and burglar alarms.

Another example is PolicyGenius, which is licensed as an independent broker in New York state and not affiliated with a particular insurer. It uses AI to provide comparisons of life insurance, long-term disability insurance, renters' insurance and pet insurance, as well as advice suited to the user. Similarly, Brolly is a mobile app that uses AI to provide insurance advice traditionally provided by an insurance broker. It also has a storage feature where the user can store all insurance policies ever purchased, as well as a shop feature where insurance cover can be purchased in seconds. Brolly is an FCA Appointed Representative of insurance brokers authorised by the FCA, Southport Insurance Brokers.[55]

A financial stability risk that may emerge is increasing interconnectedness between insurers, as there is a limited number of technology platforms supporting Big Data, for example cloud storage providers. This raises risks similar to those posed by outsourcing by banks, and the Reserve Bank may need to monitor any emergence of interconnectedness in a similar manner that it does with banks.[56]

The algorithms used in AI and robo-advice are highly technical, making it difficult to assess whether they are prone to any built-in biases and how robust they are. Any biases, which may be inadvertent and due to human error, can have a major impact, as the same algorithms may be applied to a large number of people. While the Reserve Bank‘s mandate does not extend to consumer protection, it does include promoting confidence in the insurance sector and there is the potential for any such errors to affect that confidence. There is also a risk that more sophisticated insurers may cease to provide insurance to higher risk groups, or that some consumers may not be able to access insurance at all. This could have efficiency implications, and increase the risk of high risk policyholders being concentrated in insurers that have inferior data collection or data analysis tools.

5.3 Big Data and AI: FMI

AI and Big Data can be used in retail payment systems to identify trends from the vast amounts of transaction data flowing through the systems. For example, Mastercard is using Decision Intelligence, an AI tool, to assist financial institutions increase the accuracy of real-time approvals of genuine transactions and reduce false declines.[57] Decision Intelligence

[55] https://www.heybrolly.com/, downloaded 5 October 2018.

[56] Note that there is no specific outsourcing policy in insurance; the risk management framework encompasses risks arising from outsourcing.

[57] https://newsroom.mastercard.com/press-releases/mastercard-rolls-out-artificial-intelligence-across-its-global-network/, downloaded 3 October 2018.

examines how a specific account is used over time to detect normal and abnormal spending behaviours, and leverages account information such as customer value segmentation, risk profiling, location, merchant, device data, time of day, and type of purchase made. In July 2017, Mastercard announced it had entered into an agreement to acquire a software company specialising in AI.[58] Visa also uses Big Data analytics to identify fraud opportunities.[59]

Insights gained from transaction data can be used to offer products. Mastercard has a professional services arm called Mastercard Advisors that sells insights and patterns gained from transaction data to retailers, banks, and governments.[60] SWIFT also offers a service called Business Intelligence that analyses SWIFT data to assist the customer's decision-making.[61] Paymark offers a live dashboard with insights from EFTPOS machines, including sales, revenue, and repeat customers.[62]

The use of Big Data and AI by FMIs would give them an alternative source of revenue, using data that is a by-product of their main operation as payment systems. This could have implications for the business models of those payment systems. On the one hand, the extra revenue could make them financially stronger. On the other hand, it might signal a shift of their focus away from being a payment system, with knock-on effects on innovation and competition in the payments space.

6 Digital platforms and peer-to-peer (P2P)

A digital platform can be defined in a number of ways, but for the purposes of this article, it covers the use of Internet and mobile phones to offer new products or to build a new business model. An example is P2P lending or insurance, which allows people to lend or take out insurance amongst themselves through a digital platform, such as a website, without directly engaging traditional intermediaries such as banks or insurers.

6.1 Digital platforms and P2P: Banking

Digital platforms facilitate P2P activities, such as foreign exchange and credit activity. P2P lending, also referred to as FinTech credit, involves credit activity facilitated by electronic platforms to allow borrowers to be directly matched with investors. While this has the potential to remove the need for intermediaries, the use of such platforms does not appear to be widespread at present.

P2P lending involves a prospective borrower applying for a loan on a digital platform, by providing credit information that is verified and posted by the platform. An individual loan contract is formed between the lender(s) and borrower if the prospective lender(s) decides to lend to the borrower, and the borrower's funding target is met within a predefined timeframe. The platform may facilitate the lender's decision by providing a credit risk assessment, or by auto-selecting multiple loans according to the risk and loan term preferences of the lender. The platform is not a party to the agreement, and the platform's own account is separated

[58] http://investor.mastercard.com/investor-relations/investor-news/press-release-details/2017/Mastercard-Enhances-Artificial-Intelligence-Capability-with-the-Acquisition-of-Brighterion-Inc/default.aspx, downloaded 3 October 2018.

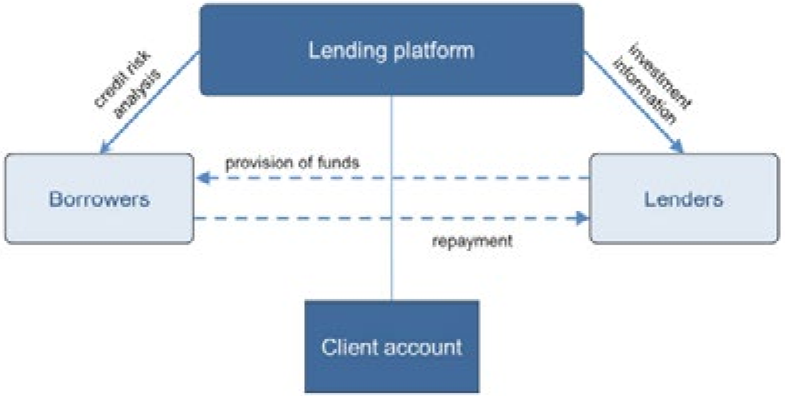
[59] https://blogs.wsj.com/cio/2013/03/11/visa-says-big-data-identifies-billions-of-dollars-in-fraud/, downloaded 3 October 2018.

[60] https://www.mastercardadvisors.com/content/advisors/en-us/about.html, downloaded 3 October 2018.

[61] https://www.swift.com/our-solutions/compliance-and-shared-services/business-intelligence/banking-insights, downloaded 3 October 2018.

[62] https://www.paymark.co.nz/products/insights/, downloaded 3 October 2018.

Figure 6
Traditional P2P lending model



Source: Financial Stability Board, 2017a

from the loaned funds and loan repayments. The platform earns revenue through fees levied on the borrowers or lenders, such as fees for account set-up, loan origination, and ongoing loan repayment. Figure 6 illustrates a basic P2P lending model:

Other forms of P2P lending include:

- the notary model, where all loans originate from banks, with the platform offering a matching service to allow banks to sell or assign the loan to creditors;
- the guaranteed return model, where the platform operator guarantees the creditors' principal and/or interest on loans;
- the balance sheet model, where lending platforms originate and retain loans on their own balance sheet; and
- the invoice trading model, where platforms offer recourse factoring.

In New Zealand, TSB Bank and Heartland Bank are involved as lenders in Harmoney, a P2P lending platform. TSB Bank has funded $50 million as an institutional investor, with the funds designated to personal lending in New Zealand,[63] while Heartland Bank has taken a shareholding stake.[64]

In Australia, legislative amendments were enacted in March 2018 to give the Australian Prudential Regulation Authority (APRA) powers over lenders who are not authorised deposit-taking institutions (ADIs) (Australian Government, 2018). APRA, like the Reserve Bank, prudentially regulates ADIs and has a mandate of financial stability, with powers to address financial stability risks posed by ADIs' lending activities. The amendments are designed to allow APRA to respond to risks to financial stability arising from lending activities by non-ADI lenders. This would cover P2P lending, which does not generally involve deposit-taking. The new powers conferred on APRA are narrow as there are no depositors to protect, and do not require APRA to prudentially regulate and supervise non-ADI lenders in the same manner as ADIs. APRA is empowered to make rules with respect to lending by non-ADI lenders to address financial stability risks, as well as a power to issue directions to a non-ADI lender.

In New Zealand, P2P lenders must be licensed by the Financial Markets Authority (FMA). There are currently eight registered P2P lending service providers[65]. A P2P lender would not fall within the Reserve Bank's

[63] http://www.interest.co.nz/business/88207/tsb-bank-says-it-has-lent-50-mln-unsecured-consumer-lending-through-p2p-lender, downloaded 3 October 2018.

[64] https://shareholders.heartland.co.nz/shareholder-resources/announcements-news/heartland-to-take-shareholding-in-harmoney,downloaded 3 October 2018.

[65] See current list at https://fma.govt.nz/compliance/lists-and-registers/licensed-peer-to-peer-lending-services/.

regulatory scope unless it falls within the definition of a bank or NBDT. At the same time, the FMA's main objective is to "promote and facilitate the development of fair, efficient, and transparent financial markets"[66]. Over the longer run, there is the potential for P2P lenders to pose risks to financial stability, which is not directly part of the FMA's remit, while such lenders may also be outside the Reserve Bank's existing regulatory perimeter.

P2P models have the potential to affect the profitability of products and services offered by banks. This may be of interest to the Reserve Bank, as an abrupt erosion of profitability may affect financial stability. Incumbent banks may also be pressured to take on more credit risk to compete with P2P lenders, as P2P lending tends to be used by borrowers who are unable to obtain credit from retail banks. This was illustrated in a 2014 survey in the UK which found that among the P2P business borrowers surveyed, 79 percent had previously sought funding from a bank, of whom 22 percent had been offered funding by the bank, while 13 percent had sought funding from a building society or credit union, of whom 3 percent had received an offer of funding (Baeck *et al*, 2014).

If P2P lending captures a significant share of credit markets, it may mitigate systemic risk to an extent, although aspects of P2P lending exacerbate risks to financial stability. P2P lending allows a lower concentration of credit in the traditional banking system, which benefits financial stability by reducing the threat traditional banks pose to financial stability. P2P lending platforms also have lower interconnectedness compared to banks. However, borrowers in some segments are placing increased reliance on P2P lending as a source of funding, and the stability of this funding has not been tested by a downturn. P2P lending could also lead to a more procyclical credit provision, as lending is affected by investors' behaviour, which may be herd-like and involve swings.

Risks identified by the Financial Stability Board (2017a) include:

- leverage: leverage in the end-investor base is likely to be smaller compared to banks, and capital resources backing the platforms' credit risks may vary.

- liquidity risk: P2P lending does not entail the same liquidity risks as banks due to investors being duration-matched and unable to exit the investment early, unless another investor takes over. However, it is possible for platforms to allow investors to access their money during the investment period, or withdraw early. This may create an expectation of easy liquidity, despite the platform not technically engaging in maturity and liquidity transformation.

- operational risk: reliance on digital platforms renders P2P lending platforms vulnerable to cyber-risk, as are third-party providers of computing services, such as cloud computing.

- quality of credit risk assessments: P2P lending platforms may have improved borrower screening through the use of Big Data analytics and better information management systems compared to banks' legacy systems.[67] However, these credit risk models have not been tested through a full credit cycle, and their impact depends on the type and quality of data the platforms use.

[66] Financial Markets Authority Act 2011, section 8.

[67] This is evidenced by TSB Bank funding loans originating from Harmoney, which uses its own credit risk assessment.

- business model incentives: There may be moral hazard risks affecting credit risk assessment in P2P lending models, where lenders rely on the platform to approve new loans to generate fee revenue, but the platform does not directly bear the credit risk of those loans, or where platforms charge higher fees to higher-risk borrowers.

- reliance on investor confidence and trust.

- low barriers to entry: P2P lending platforms tend to be less regulated compared to other financial services, with product distribution conducted online using data that are often widely available.

- securitisation: It is possible to bundle P2P credit obligations to transform them into a security, to allow them to be actively traded. Securitisation of P2P investments may create risks to financial stability by increasing the interconnectedness between P2P lending platforms, banks, and capital markets, as well as opacity for investors and regulators.

P2P lenders raise a question regarding the Reserve Bank's regulatory perimeter, which is based on deposit-taking. To the extent that P2P lending could pose risks to financial stability, for example through procyclical credit provision, the Reserve Bank may need to consider APRA's approach of regulating P2P lenders' activities. The Bank of England has expressed its view that while the P2P lending sector does not appear to pose material system risks presently, it should be monitored for slippages in underwriting standards and promotion of excessive borrowing (Carney, 2017). It has also said that the extent to which P2P lending can grow without introducing conventional risks such as maturity transformation, leverage, and liquidity mismatch, is unclear.

The relationship between P2P lending platforms and commercial banks can fragment the banking system. The provision of funding from commercial banks, for example the lending via Harmoney that is sourced from TSB and Heartland, allows commercial banks to take advantage of the P2P lending platform's screening processes, but removes loan decision-making from them at the same time. This may have implications for financial stability, as credit decision-making and screening processes are removed from regulated banks, with potentially higher credit risk, depending on the P2P lending platform's systems and processes.

An example of a digital platform in the context of RegTech is the Austrian central bank and the Austrian banking community creating a common software platform for regulatory reporting. The platform, ABACUS, is owned by a separate entity called Austrian Reporting Services GmbH, which is a company jointly owned by the seven largest Austrian banking groups representing 87 percent of the market. The platform provides a central interface between the central bank and the banks, and takes an 'input-based approach' rather than template-based reporting. The banks deliver micro-data in the form of single contracts, loans, or deposits to ABACUS in a standardised format. The data can be enriched with additional attributes and supervisors can aggregate the data without imposing additional administrative burden on the banks.

6.2 Digital platforms and P2P: Insurance

Digital platforms can be used in the insurance industry to provide insurance services through mobile phones, facilitate the provision of P2P insurance, and offer new types of products, such as pay-per-use.

An example of insurance provision through mobile technology is that provided by BIMA, a licensed insurance intermediary and/or microinsurance provider operating in 14 countries.[68] BIMA offers personal insurance products to policyholders who register using their handsets and pay by automatic deduction of prepaid airtime credit. BIMA is not licensed as an underwriter, and operates a platform to distribute and administer insurance products of its partners, or its own BIMA-branded products that are backed by an insurer.

Mobile phone applications can also be a platform for on-demand insurance. For example, Trov offers on-demand insurance for possessions that can be switched on and off through a mobile phone app, which also tracks the value of an inventory of possessions in real time. FCA-registered Cuvva also uses a mobile phone app to offer pay-as-you-go car insurance, and is reinsured by Swiss Re. Cuvva users pay a flat monthly fee of around £10 to £30 and an additional charge for each journey.

An example of P2P insurance is Friendsurance. It offers household, personal liability, legal expenses, and car insurance through policyholders of the same type forming small groups and paying a part of their respective premiums into a 'cashback pool', from where claim payments are made. If no claims are made by the end of the year, the members of the group may get up to 40 percent of their premiums from the cashback pool. Forming groups where members know each other may discourage fraudulent or exaggerated claims, and make the process transparent. Large claims are covered by normal insurers, who are partners with Friendsurance. Friendsurance currently operates as an independent broker in Germany.

Another company using a similar model is Lemonade: premiums are paid into a claims pool, from which claims are paid out after taking out monthly fixed fees for reinsurance coverage and expenses. If the total of premiums exceeds the fees and paid claims, an annual 'Giveback' is returned to the policyholders to be donated to charities of the group's choice. If the claims exceed the size of the pool, reinsurance is used to pay for the claims. Premiums are calculated on an individual basis, using a number of different factors such as credit history and information about the property. Lemonade works with reinsurance partners.

If P2P insurance models emerged in New Zealand, the issue for the Reserve Bank could be whether the particular P2P insurance model/structure is considered to be a contract of insurance and therefore regulated, or not, as the case may be. To be captured under the Insurance (Prudential Supervision) Act 2010 (IPSA), the offering would need to fall within the definition of a contract of insurance, where there is acceptance of risk in return for a premium. Some variations of P2P insurance models that have appeared overseas appear to have mutual characteristics and may even be discretionary in nature, with some or all of the risk being borne by the members, and would therefore potentially fall outside the current scope of IPSA if they operated in New Zealand.

P2P insurance models and microinsurance can encourage competition and growth in the insurance sector. This has led to overseas regulators,[69] including central banks, developing forums to encourage this competition and to pre-empt issues that might arise from a regulatory perspective by engaging with innovators. While greater competition is a matter of interest for the Reserve Bank given the efficiency part of its mandate, implementation of platforms to encourage competition may fall principally

[68] Ghana, Senegal, Tanzania, Bangladesh, Cambodia, Indonesia, Pakistan, Philippines, Sri Lanka, Fiji, Papua New Guinea, Haiti, Honduras, and Paraguay.

[69] FCA's Innovation Hub (UK), Monetary Authority of Singapore's regulatory sandbox, Australian Securities and Investment Commission's Innovation Hub, HKMA, Ontario Securities Commission.

within the responsibilities of the Commerce Commission, Ministry of Business, Innovation and Employment, or the Productivity Commission. If the Reserve Bank were to encourage microinsurance initiatives, it may want to consider how this might be best facilitated, such as possible exemptions or relief from certain licensing requirements. Any relief needs to balance the benefits of the different types of products that are facilitated by digital platforms, together with any different risks compared to traditional products and models.

Another development facilitated by digital platforms is the use of cloud computing in back-end systems by insurers. For example, InsuredHQ, based in New Zealand, offers a full policy, client, accounts and claims management system designed for insurers. The system allows individual underwriting of risk, facilitating microinsurance. It has attracted the attention of large insurers looking to replace their server-based legacy systems with cloud-based systems,[70] which may lead to risks of interconnectedness arising from the use of a single big provider by many insurers.

6.3 *Digital platforms and P2P: FMI*

Digital platforms can be used for payments, for example through digital wallets and e-money. 'Digital wallet' refers to software that stores the user's bank or credit card account information and provides it to the seller when the user buys something on the Internet. 'E-money' refers to an electronic store of monetary value on a technical device that may be widely used for making payments to entities other than the e-money issuer.[71]

In New Zealand, a 2017 survey of more than 1000 New Zealanders by Mastercard found that one in 10 respondents have used a digital wallet when shopping online. Mobile digital wallet services currently available in New Zealand are Android Pay (BNZ), Apple Pay (ANZ and BNZ), ANZ goMoney Wallet, and ASB Virtual. Semble, a joint venture between ASB, ANZ, Vodafone, and Spark, discontinued its digital wallet which allowed the user to wave their phone on an EFTPOS terminal to make payments.[72]

The use of digital wallets can threaten banks by depriving them of customer information from payments, but can also present an opportunity for banks as they have a competitive edge in being positioned to simplify the process of transferring money between conventional bank accounts and digital wallets.

In the UK, the Digital Economy Act 2017 extends the definition of payment system to allow the HM Treasury to recognise non-interbank payment systems for oversight by the Bank of England under the Banking Act 2009. HM Treasury may designate a systemically important non-bank payment system to be supervised by the Bank of England. It also empowers HM Treasury to apply the existing Settlement Finality regime to non-bank payment service providers. This means that if those providers become insolvent, preferential treatment concerning Settlement Finality applies, which ensures the provider's unsettled transactions within the system are settled (UK Government, 2017).

The Bank of England has also widened access to central bank money to non-bank payments service providers, by allowing them to apply to access the Bank of England's RTGS system. This initiative supports the Bank of England's view that diversification is good for stability, as the

[70] http://www.insurancebusinessmag.com/nz/news/breaking-news/kiwi-tech-providers-micro-insurance-mission-going-global-52168.aspx, downloaded 3 October 2018.

[71] As defined by the European Central Bank – https://www.ecb.europa.eu/stats/money_credit_banking/electronic_money/html/index.en.html

[72] https://www.nbr.co.nz/article/semble-put-sleep-ck-194136, downloaded 3 October 2018.

existing system creates single-point-of-failure risks due to its tiered and highly concentrated nature. The Bank of England has also expressed the view that it would be possible for traditional bank-based payment services and systems to be displaced by virtual currencies and FinTech-based providers, particularly where they gain direct membership to central bank systems (Carney, 2017).

In Australia, APRA regulates PayPal Australia, a purchased payment facilities provider that provides digital wallets, as an ADI.

In Hong Kong, stored value facilities are subject to a licensing regime administered by the HKMA. A stored value facility is defined (Hong Kong Monetary Authority, 2015) as a facility that:

- may be used for storing a value of an amount of money that is paid into the facility from time to time; and
- may be stored on the facility; and
- may be used for the purpose of making payments for goods or services under an undertaking given by the issuer; and/or
- may be used as a means of making payments to another person under an undertaking given by the issuer; and
- includes both device-based and non-device based (i.e. network-based) stored value facilities.

Device-based: stores value in an electronic chip on a card or physical device

Non-device based: stores value on a network-based account which can be accessed through the Internet, computer network, or mobile network.

The HKMA decides whether a licence should be issued, and conducts ongoing supervision of licensees, including conducting investigations and imposing sanctions on licensees where appropriate. Current licensees include TNG (Asia), which offers e-wallets, and Octopus Cards, which offers cards or ornaments that can be used to pay for transport, parking, goods and services from participating shops, leisure facilities, hospitals, public services, and schools.

In Europe, the E-money directive sets out the rules for e-money services in the EU. E-money covers cashless payments using money stored on a card or a phone, or over the internet. The directive facilitates newcomers to the e-money market by setting prudential rules proportional to the risks faced by e-money institutions,[73] while protecting consumers by requiring safeguarding of consumer funds. Consumer funds must be deposited in a separate account from any other activities conducted by the operator, or invested in secure low-risk assets, with protection from creditors or covered by an insurance policy.

The Reserve Bank does not regulate stored value facilities in the manner of HKMA. The Non-bank Deposit Takers (Declared-out Entities) Regulations 2015 exempts payment facility providers from the Non-bank Deposit Taker Act 2013 in certain circumstances, and this would include e-money such as Snapper cards[74]. This reflects the differences in regulatory philosophy as well as the size and importance of payment facility providers in Hong Kong and New Zealand. For example, in Hong

[73] For example, reducing the initial capital requirement to 350,000 euros (from 1 million euros) and new rules on calculating own funds. https://www.lexology.com/library/detail.aspx?g=e03f2a34-3e5e-479a-b33b-5dddd709b317

[74] Snapper cards are used for payment on public transport in Wellington.

Kong the Octopus Card is accepted by more than 20,000 retail outlets and more than 9,000 service providers, more than 99 percent of people aged 15-64 have one, and over 14 million transactions are processed a day.[75]

While there is currently no payment facility provider in New Zealand large enough to be supervised as an FMI, there would be scope for supervision under the new FMI framework if a payment facility provider became significant enough to be designated.

7 Other developments

Other technological developments that may be categorised as 'FinTech' include:

'gamification': the use of game elements to influence behaviours of individuals, for example prizes, points, teamwork, and scorekeeping. Gamification may motivate users to meet specific goals, enhance customer engagement, and encourage behaviours that reduce risks to safe driving and health.

augmented reality: superimposing a computer-generated image on a user's view of the real world, for example Pokemon Go. In the banking context, National Bank of Oman has released an Augmented Reality app[76] that provides information on branches, ATMs, and offers as the user moves the mobile phone around to capture the surroundings on the mobile phone camera. PayPal has filed a patent for the use of augmented reality in paying for an item that is seen through a device, such as purchase of bus fares from merely viewing a bus through an augmented reality headset.

virtual reality: simulated environment created by computer technology. For example, Citibank's traders use a Holographic Workstation, where users can see data as 3D images and interact with the data using hand and voice commands. MasterCard has also developed a prototype that allows users to identify an item within MasterCard's virtual reality golf experience, and buy it without leaving the virtual world.

drones: unmanned aircraft or ship guided by remote control or on-board computers. Drones may be used to enhance insurance assessments.

robots: includes autonomous cars, that could affect insurers through motor insurance no longer being directed at drivers.[77]

3D printing: also called additive manufacturing, involves the making of a three-dimensional physical object through layering of material under computer control. It may affect insurers by raising a question regarding product liability, for example by end-users being able to complete a product.[78]

biometric technologies: the measurement and analysis of unique physical or behavioural characteristics, for example fingerprint or voice, as a means of verifying personal identity. Biometrics can be used for

[75] http://www.octopus.com.hk/octopus-for-businesses/benefits-for-your-business/en/index.html, downloaded 3 October 2018.

[76] https://www.nbo.om/en/Pages/Personal-Banking/Support/Augmented-Reality-App.aspx , downloaded 3 October 2018.

[77] http://www.npr.org/sections/alltechconsidered/2017/04/03/522222975/self-driving-cars-raise-questions-about-who-carries-insurance , downloaded 3 October 2018.

[78] http://www.swissre.com/reinsurance/insurers/engineering/3D_printing_implications_for_the_reinsurance_industry.html, downloaded 3 October 2018.

security and identity protection. Although it is beyond the scope of this article, biometrics may have AML/CFT uses.

8 Cyber risk

Cyber risk is one of the 10 issues arising from FinTech that the Financial Stability Board (2017) has identified as meriting the attention of authorities.[79] Unlike other types of operational risk, capital requirements cannot ameliorate cyber risk as capital is insufficient to restore operations in the face of a cyber-attack. FinTech innovations can exacerbate cyber risk, while certain aspects of FinTech can address cyber risk.

Greater connectivity between institutions and FinTech firms may exacerbate cyber risk by increasing the number of points of access and hence the number of potential weak links. For example, banks partnering with P2P lending platforms may be exposed to cyber risk from the digital platform used for P2P lending. Reliance on common hosts for cloud computing or data storage may render banks and insurers vulnerable to single point of failure risks and interconnectedness.

FinTech firms also tend to derive competitive advantage from releasing products earlier than competitors, which may lead to premature adoption of technologies without adequate testing and safeguards. Mobile devices and internet of things are vulnerable to cyber-attacks if they do not contain anti-virus software. Symantec's analysis of 10.8 million mobile phone apps classified 3.3 million apps as malware, 3 million apps as grayware, and 2.3 million apps as madware.[80]

Greater collection and sharing of data also leads to more serious consequences from breaches, and sharing of data across a wider set of parties can make protection of data and systems more difficult. Cyber-attacks that result in loss or leakage of customer information can erode trust and cause financial damage.

FinTech may also be used to facilitate cyber-attacks. For example, crypto-currencies such as bitcoin have been specified by cyber attackers as the preferred mode of payment for cyber-attack ransoms.[81] There are also reports of a cyber-attack that infects computers to mine crypto-currency by installing a currency 'miner' without the user's knowledge. The attack allows computers to operate while mining for crypto-currency in the background.

On the other hand, cyber risk may be mitigated by aspects of FinTech. If FinTech leads to diversification in the type of providers, failure in one type of institution, for example banks, is unlikely to bring the market to a standstill. Increasing diversity and competition may lessen the impact of a single cyber-attack. Replacement of legacy systems may also reduce cyber risk, although the use of cloud computing may introduce new points of attack. As discussed in section 2.3, decentralised DLT may lessen the impact of a cyber-attack by maintaining multiple copies of the ledger.

[79] The 10 issues are: managing operational risks from third party service providers; mitigating cyber risks; monitoring macrofinancial risks; cross-border legal issues and re™gulatory arrangements; governance and disclosure frameworks for big data analytics; assessing regulatory perimeter and updating it on a timely basis; shared learning with a diverse set of private sector parties; further developing open lines of communication across relevant authorities; building staff capacity in new areas of required expertise; and studying alternative configurations of digital currencies.

[80] Malwares are programs created to do harm, e.g. computer viruses, worms, and Trojan horses; graywares are programs that do not contain viruses but can be annoying or harmful to the user, e.g. hacking tools, accessware, and spyware; madware are aggressive techniques to place advertising in the mobile device's photo albums, calendar entries, and notifications (Symantec, 2016).

[81] For example, the WannaCry ransomware demanded a ransom of $300 worth of bitcoin to unlock the contents of the infected computer. An earlier version, WeCry asked users for 0.1 bitcoin to unlock the files and programs of the infected computer.

9 Conclusion

FinTech has the potential to change the landscape of the financial sector by introducing new products and services, new business models and more competition for incumbents. This has the potential to enhance financial sector efficiency, but it also raises questions about financial sector stability.

The emergence of FinTech creates new market opportunities that could benefit consumers, improve financial system resilience and might even lead to more efficient regulation. This is to be welcomed and should be encouraged by regulators where possible. Prudential regulation does not create any obstacles to the adoption of innovative FinTech solutions in New Zealand as far as the Reserve Bank is aware, and the Reserve Bank engages with industry and other New Zealand regulators to gauge whether there is a role for regulation in facilitating FinTech innovation more generally.[82]

But FinTech also creates new risks which pose new challenges for the Reserve Bank and other regulators. Some of the emerging technologies allow fragmentation of the value chain of activities carried out by the firms that are currently supervised by the Reserve Bank. For example, FinTech has the potential to unbundle banking into its core functions of settling payments, performing maturity transformation, sharing risk, and allocating capital. It could undermine the position of incumbents through a loss of business, or reduced access to information or liquidity, and lead to the emergence of new systemically important players.

In future, there may be a need for prudential regulation to respond to these developments. Supervision of existing supervised entities may need to adapt. But beyond that, if the Reserve Bank is to continue to promote the stability and efficiency of the financial system, there may need to be a re-drawing of the perimeter defining which types of activity, and which classes of entity involved in those activities, should fall within the Reserve Bank's prudential supervision.

At this stage, however, FinTech developments have had only a limited impact on the financial sector, and new risks that have arisen as a result are minimal and contained. For the time being, the appropriate response by the Reserve Bank appears to be enhanced monitoring of emerging FinTech developments, which might require better data collection, and continued engagement with industry and other regulators.

[82] The Reserve Bank does not currently see a need for any formal 'sandbox' arrangements (Reserve Bank of New Zealand, 2017).

Appendix

FinTech implications for the Reserve Bank mandate, organised by sector

(1) Banking

Technology	*Impact on Reserve Bank's mandate*
DLT, blockchain, and smart contracts	Efficiency: • A DL (under most designs) creates a single, true record across banks, eliminating the need for reconciliation. • Smart contracts could be used to automate the performance of contracts. • However, the verification process in DLT could involve significant computational costs. • Implementation of DLT may be hindered by difficulties in incorporating, or replacing, banks' existing legacy systems with DLT. Stability: • Resilience from attack.
Crypto-currency	The Reserve Bank may need to respond if the use of crypto-currencies becomes widespread and extends beyond the mere buying and selling of them as a commodity, for example into lending activities. This seems unlikely at present, as crypto-currencies face AML/CFT difficulties in New Zealand.
API	Efficiency: • Open banking and aggregators can improve efficiency by allowing customers to be matched with the best rates and make informed decisions, but it may be an initiative that is better suited to the Commerce Commission or MBIE, rather than the Reserve Bank. Stability: • If banks are initiating collaboration with developers using APIs to create customer-facing apps, there may be risks around data protection or use of apps without adequate testing, but it is unlikely that banks would allow third parties to usurp their core functions. • Open banking may have financial stability implications if it creates more customer churn, resulting in weaker, more arms-length client relationships. Deposits may become less stable and increase liquidity risk. Prudential standards may need to be adjusted. • Note that Payments NZ's current investigation of APIs in its Payments Direction programme includes registered banks. RegTech: • APIs could be used to access banks' information as needed, without the need for private reporting. • The Reserve Bank's Banking Supervision Handbook could also be made more accessible.

Big Data and AI	Efficiency: • Machine learning can improve the efficiency of decision-making processes, but algorithms may require a development of monitoring and auditing standards for algorithms in AI. • Use of AI in credit decisions may require the Reserve Bank to inquire into algorithms in a similar manner to internal models, and demand specialised Reserve Bank resources. • Significant privacy, data protection, and consumer protection concerns may hamper implementation. Stability: • Big Data is facilitated by cloud computing, which provides scalable on-demand processing and storage for data. Data storage is regulated by the laws and regulations in the country where the storage is located, and multiple institutions may use a common provider. • The use of robo-advice in trading and investment falls within FMA's jurisdiction, but the Reserve Bank may respond where widespread use of robo-advice may impact financial stability through errors or disruptions in algorithms across robo-advisors with significant market share, leading to systemic implications. RegTech: • Big Data can be used to identify trends in systemic risk and economy. • AI may be used to enforce regulatory compliance.
Digital platforms and P2P	Stability: • Non-deposit-taking P2P lenders may need to be brought within the Reserve Bank's regulatory perimeter if they pose risks to financial stability. • P2P models can erode banks' profitability. • Incumbent banks may also be pressured to take on more credit risk to compete with P2P lenders. • If P2P lending captures a significant share of credit markets, P2P lending could lower the concentration of credit in the traditional banking system. • P2P lending platforms have lower interconnectedness compared to banks. • However, the stability of P2P funding has not been tested by a downturn, and P2P lending could lead to more procyclical credit provision. • Other changes in risk identified by the FSB are in the areas of leverage, liquidity risk, cyber-risk, the quality of credit risk assessment, the level of regulation, and risks arising from securitisation of PS2P lending. RegTech • Digital platforms could be used to create a common software platform for regulatory reporting.
Other developments	• Augmented reality has been used for banking apps. • Biometric technologies can be used for security and identity protection. Although it is beyond the scope of this article, biometrics may have AML/CFT uses.

(2) Insurance

Technology	*Impact on Reserve Bank's mandate*
DLT, block-chain, and smart contracts	There is no immediate need for a response by the Reserve Bank, but future developments may include: • possible efficiency gains; • emergence of non-traditional companies from lower barriers to entry; • potential increase in liquidity risk from increased claims efficiency; and • use of DAOs (Digital Autonomous Organisations) raising questions of who is responsible for regulatory compliance.
Crypto-currency	Crypto-currencies do not appear to have significant implications for the insurance industry.
APIs	APIs are used in conjunction with other technologies, and may enhance efficiency.
Big Data and AI	Stability: • Insurers may become more interconnected, due to the limited number of platforms supporting Big Data. • Algorithms used in AI and robo-advice are unlikely to be transparent, with potential built-in biases leading to unethical or inappropriate advice. The impact of human error in an algorithm may be magnified because it is applied to many people. • The use of Big Data to exclude higher risk customers may mean that insurers with inferior data collection or data analysis tools end up with a larger share of high-risk policyholders.

Digital platforms and P2P	P2P insurance model raises the question of whether a P2P insurance platform is an ‘insurer’ in terms of IPSA, and whether it should nonetheless be regulated. Efficiency: • P2P insurance models and microinsurance can encourage competition in the insurance sector. However, implementation of platforms to encourage competition may be better suited for the Commerce Commission, MBIE, or the Productivity Commission. • If the Reserve Bank were to encourage microinsurance initiatives, it could consider how this might be best facilitated, for example by exemptions or relief from certain licensing requirements. However, the risks differ from those of traditional products and models. Stability • Different types of products facilitated by digital platforms can carry different risks to traditional products. • Use of cloud computing in back-end systems by insurers may lead to risks of interconnectedness from the use of a single big provider by many insurers.

Other developments	• Gamification can incentivise behaviours that reduce risks to safe driving and health. • Drones may be used to enhance insurance assessments. • Autonomous cars could affect insurers, as motor insurance would no longer be directed at drivers. • 3D printing may affect insurers by raising a question regarding product liability, for example by end-users being able to complete a product.

(3) Financial Market Infrastructures (FMIs)

Technology	*Impact on Reserve Bank's mandate*
DLT, blockchain, and smart contracts	Efficiency: • Enhance efficiency by speeding up transactions and reducing settlement time for wholesale and international payments. • However, many of the benefits of DLT, such as faster settlement, may be achievable through traditional technology. The current speed reflects market preference, rather than technological constraints. Stability: • Unpermissioned DLT could reduce systemic operational risk by reducing the financial system's reliance on a centralised third party, creating a number of contributors maintaining back-ups, and enhancing resilience to cyber-attacks. However, the vulnerability of DLT to cyber-attacks depends on its design. • If a new FMI based on DLT emerges, it is likely to be non-systemic and not subject to standards set by the Reserve Bank in its early stages. • If an FMI based on DLT subsequently grows to become systemic, it would become subject to prudential standards. (The proposed new legislative framework for FMIs will define the threshold for being deemed systemic.) • The Reserve Bank may need to ensure that the standards it imposes on FMIs are adequate to cover risks specific to DLT, which may differ to those of traditional systems. This may require work to understand the risks before developing standards.
Crypto-currency	Widespread adoption of crypto-currencies, for example in cross-border transactions, would reduce FMIs' role.
API	APIs can be used in payment systems to enhance interoperability across different systems.
Big Data and AI	Use of Big Data and AI for alternative source of revenue from data insights may raise financial stability concerns if FMIs become reliant on this alternative source of revenue to the extent that the profitability of Big Data operations affect the provision of critical functions.
Digital platforms and P2P	There are currently no payment facility providers large enough to be supervised as an FMI. There is scope for supervision under the new FMI framework if a payment facility provider becomes significant enough to be designated.
Other developments	Virtual reality can incorporate payment systems within the virtual world.

References and other background material

Addleshaw Goddard LLP (2017) 'InCredit – 16 May 2017' Lexology. https://www.lexology.com/library/detail.aspx?g=f4a40f4b-fa40-4c92-9f8a-59a42d8d7595

Ali R, Barrdear J, Clews R and Southgate J (2014) 'The economics of digital currencies' *Bank of England Quarterly Bulletin*, 2014 Q3, pages 276-286

Ali R, Barrdear J, Clews R and Southgate J (2014a) 'Innovations in payment technologies and the emergence of digital currencies' *Bank of England Quarterly Bulletin*, 2014 Q3, pages 262-275

Australian Government (2017). 'Review into Open Banking in Australia – Issues Paper'. https://static.treasury.gov.au/uploads/sites/1/2017/08/Review-into-Open-Banking-IP.pdf

Australian Government (2018) 'Treasury Laws Amendment (Banking Measures No. 1) Act 2018'.

Baeck, P, L Collins and Z Zhang (2014), 'Understanding Alternative Finance: The UK Alternative Finance Industry Report 2014', Nesta, London – https://www.nesta.org.uk/report/understanding-alternative-finance-the-uk-alternative-finance-industry-report-2014/

Bank of Canada (2017), 'Project Jasper: Are Distributed Wholesale Payment Systems Feasible Yet?', *Financial System Review*, June 2017.

Bank of England (2017). 'Bank of England extends direct access to RTGS accounts to non-bank payment service providers' Press release, from https://www.bankofengland.co.uk/-/media/boe/files/news/2017/july/boe-extends-direct-access-to-rtgs-accounts-to-non-bank-payment-service-providers.pdf

Brignall, M (2017) 'Pay-as-you-go car insurance – perfect for the low-mileage driver?', *The Guardian*, 11 February 2017,.https://www.theguardian.com/money/2017/feb/11/pay-as-you-go-car-insurance-low-mileage-driver-cuvva-just-miles

Broadbent, B (2016) 'Central banks and digital currencies', speech given at London School of Economics.

Carney, M (2017) 'The Promise of FinTech – Something New Under the Sun?', speech given at Deutche Bundesbank G20 conference on 'Digitising finance, financial inclusion and financial literacy', Wiesbaden.

Carney, M (2017a) 'Building the Infrastructure to Realise FinTech's Promise', speech given at International FinTech Conference 2017, Old Billingsgate

Chiu, J and Koeppl, T (2017) 'The Economics of Cryptocurrencies – Bitcoin and Beyond'.

Cognizant (2017) 'Blockchain: A Potential Game-Changer for Life Insurance'.

Committee on Financial Markets, Directorate for Financial and Enterprise Affairs (2017) 'Understanding the Digitalisation of Financial Services: A Framework for Financial Regulators' Organisation for Economic Co-operation and Development DAF/CMF(2017)6

Committee on Payments and Market Infrastructures (2017) ‘Distributed ledger technology in payment, clearing and settlement – an analytical framework’. Bank for International Settlements.

Cuber (2015) ‘Conditions of use of the CUBER APP during the test period’.

Ergürel, D (2016) ‘How virtual and augmented reality can transform the future of FinTech?’ Haptical from https://haptic.al/how-virtual-and-augmented-reality-can-transform-the-future-of-fintech-3c52b0a79c34

EUR-Lex (2016) ‘Electronic money: business and prudential supervision’ Document 32009L0110. http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32009L0110

European Commission ‘E-money’. https://ec.europa.eu/info/business-economy-euro/banking-and-finance/consumer-finance-and-payments/payment-services/e-money_en

Financial Conduct Authority (2017) ‘Discussion Paper on distributed ledger technology’ DP17/3.

Financial Stability Board (2017) ‘Financial Stability Implications from FinTech – Supervisory and Regulatory Issues that Merit Authorities’ Attention’

Financial Stability Board (2017a) ‘FinTech credit: Market structure, business models and financial stability implications’

Gray, M (2016) ‘NZ P2P insurance fails to fly’ Insurance Business NZ.

Hong Kong Monetary Authority (2015) ‘Explanatory Note on Licensing for Stored Value Facilities’. Accessed from http://www.hkma.gov.hk/eng/key-functions/international-financial-centre/regulatory-regime-for-svf-and-rps/regulation-of-svf.shtml

Insurance and Private Pensions Committee, Directorate for Financial and Enterprise Affairs (2016) ‘Draft report on technology and innovation in the insurance sector’ Organisation for Economic Co-operation and Development DAF/AS/WD(2016)13

International Association of Insurance Supervisors (2017) ‘FinTech Developments in the Insurance Industry’.

International Monetary Fund (2017) ‘Fintech and Financial Sevices: Initial Considerations’ IMF Staff Discussion Note SDN/17/05.

Kumar, A and Smith, C (2017) ‘Crypto-currencies – An introduction to not-so-funny moneys’, Reserve Bank of New Zealand Analytical Notes, AN2017/07

Lomas, N (2015) ‘Everledger is Using Blockchain to Combat Fraud, Starting with Diamonds’.

Menn, J (2017) ‘Hackers mint crypto-currency with technique in global ‘ransomware’ attack’ from http://www.reuters.com/article/us-cyber-attack-cryptocurrency-idUSKCN18D00W

Morgan, P (2017) ‘Bitcoin, Blockchains, Smart Contracts: For Lawyers – The Blockchain.NZ’ Blockchain Labs, from https://youtu.be/sdBDmfseWjQ

Nawijn, B (2017) '9 Applications of AR & VR in the Financial Industry' TJIP from https://www.tjip.com/publicaties/9-applications-of-ar-vr-in-the-financial-industry

Payments UK (2016) 'The Second Payment Services Directive (PSD2) – A briefing from Payments UK'

PwC (2017) 'The FinTech survey 2017'

PwC (2016) 'Blockchain – an opportunity for energy producers and consumers?' from https://www.pwc.fr/fr/assets/files/pdf/2016/12/blockchain_opportunity_for_energy_producers_and_consumers.pdf

Reserve Bank of New Zealand (2017) *Financial Stability Report* November 2017, Box C https://www.rbnz.govt.nz/financial-stability/financial-stability-report/fsr-november-2017/fintech-developments-and-implications-for-rbnz-regulatory-responsibilities

Swiss Re Institute (2017) 'Technology and insurance: themes and challenges'.

Symantec (2016) 'Internet Security Threat Report' from https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

The FinTech 50 (2016). 'The FinTech 50 2016 – The fifty hottest FinTechs in Europe'.

Transatlantic Policy Working Group FinTech (2017) 'The Future of RegTech for Regulators – Adopting a Holistic Approach to a Digital Era Regulator'

UK Government (2017) 'Explanatory Notes – Digital Economy Act 2017' http://www.legislation.gov.uk/ukpga/2017/30/pdfs/ukpgaen_20170030_en.pdf

UK Government Chief Scientific Advisor (2016) 'Distributed Ledger Technology: beyond block chain' https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain

Venter, C (2016) 'ANZ's Christian Venter details nine reasons why banks aren't using blockchain' http://www.interest.co.nz/business/81499/anzs-christian-venter-details-nine-reasons-why-banks-aren%E2%80%99t-using-blockchain

Wadsworth, A (2018), 'What is digital currency?' Reserve Bank of New Zealand *Bulletin*, 81(3).

Wadsworth, A (2018a), 'Decrypting the role of distributed ledger technology in payments processes' Reserve Bank of New Zealand *Bulletin*, 81(5).

Wadsworth, A (2018b), 'The pros and cons of issuing a central bank digital currency' Reserve Bank of New Zealand *Bulletin*, 81(7).

Watson, A (2016) 'Disruption or distraction? How digitisation is changing New Zealand banks and core banking systems', Reserve Bank of New Zealand *Bulletin*, 79(8).