The Potential and Perils of Financial Technology: Can the Law adapt to cope?

The First Edinburgh FinTech Law Lecture, University of Edinburgh

Lord Hodge, Justice of the Supreme Court

14 March 2019

"Money is fine, Arron, but data is power". That is a fictional quotation. But it contains an important truth.

The playwright, James Graham, put those words, or words to that effect, into the mouth of Dominic Cummings in a fictional conversation with Arron Banks, the businessman who has funded UKIP and the leave campaign in the Brexit referendum.[1] Data is power. So is artificial intelligence. And the theme of my talk this evening is whether, and if so how, law and regulation can cope with the challenges which the use of data and AI by the financial community is posing.

There are four technological developments which have created the new opportunities and challenges. They are, first, the huge increase in the computational and data processing power of IT systems. Secondly, data have become available on an unprecedented scale. Thirdly, the costs associated with the storage of data have fallen. And, fourthly, increasingly sophisticated software services have come onto the market.

There are various definitions for Artificial Intelligence, or AI, which focus on its ability to perform tasks that otherwise would require human intelligence. Jacob Turner, in his recent book on regulating AI, called "Robot Rules" speaks of AI as "the ability of a non-natural entity to make choices by an evaluative process".[2] That is so, but AI is not confined to matching human intelligence in the performance of its tasks. Machines can beat grand masters at chess and outperform expert players of "Go".[3] I would prefer to define AI as computer systems able to perform tasks which traditionally have required human intelligence or tasks whose completion is beyond human intelligence.

[1] The Channel 4 drama, "Brexit: the uncivil war", which was initially released on 7 January 2019.

[2] Jacob Turner, "Robot Rules: regulating artificial intelligence" (2019) p 16.

[3] In 1997 IBM's Deep Blue defeated Gary Kasparov at chess and in 2016 Google DeepMind's AlphaGo program beat the 18-time world champion Lee Sedol.

Within AI, there is machine learning, which involves the designing of a sequence of actions to solve a problem, known as algorithms, which optimise automatically through experience and with limited or no human intervention.[4] This ability poses significant challenges to our law, as I will seek to show.

There is also the process known as "big data analytics". Computers can now find patterns in large amounts of data from many and diverse sources. And our data is readily available. In 2016 68% of adults in the eleven most economically advanced countries owned a smart phone, giving access to the Internet and machine learning. It is a great empowerment. But it has its downside. As Jacob Turner stated: "Every time we use a search engine, that search engine is using us".[5] It raises major questions about our privacy and about manipulation of decision-making via the use of targeted advertising or other pernicious uses of social media, as recent concerns about the misuse of Google and Facebook have shown.

There are many benefits from the new innovations, and, in particular, the new processing capacity and storage infrastructure. The new capacity can be used beneficially in the diagnosis of diseases, the translation of foreign languages and the development of driverless vehicles. Law enforcement authorities increasingly use these techniques to both detect and deter crime early. It will also prove a very useful when authorities decide on the likelihood that a person will re-offend. Durham police have been experimenting with the use of computerised harm assessment risk tool to give guidance on whether an alleged offender should be kept in custody or be given bail. Scientists in the USA advocate the wider use of these techniques. The United Nations Global Pulse has an interesting initiative using machine learning in combination with natural language processing to analyse material on the web, in social media, in newspapers and from other sources to assess the effectiveness of policies and to detect and anticipate emerging socio-economic or political problems.

[4] These definitions are taken from a paper by the Financial Stability Board, "Artificial intelligence and machine learning in financial services" (1 November 2017).

[5] Turner (fn 1), p 23.

There are also less benign uses to which big data analytics and AI can be put. They can be used as a method of social control by authoritarian regimes in ways which pose serious challenges to Western concepts of human rights. In China, the government is developing a "social credit system" using big data analysis technology to assess the economic and social reputation of its citizens and businesses with the aim of promoting trust. But it is a very wide-reaching mechanism. As a result, it can involve the blacklisting of debtors who do not implement court judgments; it can also penalise mere social behaviour which the algorithm deems as not conducive to promotion of trust or "good citizenship". The scoring extends to the mining of people's data on websites to get a full profile of their behaviour including their friends, their health, the newspapers they read, their shopping history and their social exchanges. The system awards credits for approved behaviour and negative credits for behaviour that is frowned upon. People with low credit scores can be registered on a public blacklist and excluded from high speed trains or banned from domestic flights[6] and there are reports of people being refused access to hotels, to private schools and exclusion from prestigious work.

In western society, governments have not sought to exercise such control but there are concerns about the potential for abuse of big data, for example, in relation to access to health insurance or to credit. And there is widespread concern about the misuse of data by tech giants such as Facebook and Google. Concerns about foreign intervention in our democratic processes have grown. While I know that it is statement by the prosecution, the Grand Jury's indictment in *United States v Internet Research Agency LLC* dated 16 February 2018, which is a product of the enquiry by Special counsel, Robert Mueller, is a sobering read, giving an account of the employment of hundreds of individuals and the expenditure of millions of dollars on online operations, the creation of fictitious persons as opinion formers, and the carrying on of a misinformation operation on YouTube, Facebook, Instagram and Twitter to spread distrust of presidential candidates and the political system in the lead up to the 2016 Presidential Election.

The speed of technological development poses a real challenge to the law and to regulation. The business consultancy, McKinsey has estimated that, compared with the Industrial Revolution, the changes being effected by AI are happening ten times faster and at 300 times the scale, thus

[6] "The Guardian" (Lily Kuo) reported on 1 March 2019 that by the end of 2018 the Chinese courts had banned would-be travellers from taking flights 17.5 million times and travel bans by train had been imposed 5.5 million times. In 2018 alone 6.15 million citizens were banned from taking flights.

having roughly 3000 times the impact.[7] The McKinsey Global Institute highlights the increasing pace of technological change and quotes an estimate from an industry insider that humankind will generate more data in the next five years than it has created in five thousand years.[8] It is necessary to ask: can the law cope?

Fintech

My topic today is not so much these wider concerns but the more focused question of the use of AI, big data and other financial technology by financial firms. Many of the concerns about the wider use of AI and big data are replicated in the world of Fintech. I will examine some of the benefits or potential benefits of Fintech, before looking at blockchain technology, AI and machine learning, and data protection. Then I will seek to set out some ideas on the need to reform the law of contract to address smart contracts and contracts created between machines, the attribution of responsibility in delict (tort) for harm caused by semi-autonomous or autonomous machines, and the development of new concepts in property law. Finally, I will ask how this is to be done and make some observations concerning regulatory initiatives.

The power of AI and machine learning to analyse data should be able to contribute to a more efficient financial system in those economies which embrace Fintech. Lenders will have more information to assess the credit quality of borrowers and to make decisions on whether and how much to lend quickly. Insurers will better be able to assess risk and market their insurance contracts more efficiently. Customers of financial institutions increasingly rarely visit their bank branch but obtain money from ATMs and, if they have the patience to do so, solve problems by speaking to "chatbots" (which are computer programs which simulate conversations with human customers in natural language). Banks are thus able to provide their services with many fewer staff and branches.

Banks are using AI and machine-learning to maximise profits from scarce capital, to improve their models for risk-management and stress-testing, and to carry out market impact analysis, by creating so-called "trading robots" which evaluate the impact of the business's own trading on

[7] Fn 2 p 35.

[8] Dobbs, Manyika and Woetzel, "No Ordinary Disruption: The Four Global Forces Breaking All Trends" (McKinsey Global Institute) 2015, ch 2: 'The Tip of the Iceberg: Accelerating Technological Change', pp 33-41.

the market in which it operates. Asset managers and trading firms can use machine learning to devise trading and investment strategies and, in portfolio management, to predict price movements.

Advocates of Fintech assert that consumers and investors should benefit from lower fees and borrowing costs if the new technology reduces the cost of financial services. The technology also has the potential to make financial services available to consumers who are currently excluded from or have only limited access to such services, for example because of having no credit profile. Access to reasonably priced credit can do much to alleviate poverty, both at home and internationally.

DLT

The development of algorithms has enabled the collaborative creation of digital distributed ledgers by which a database of assets is shared across a network of sites, geographies and institutions and in which all participants have their own identical copy of the ledger.

The European Securities Markets Authority[9] has described Distributed Ledger Technology ("DLT") systems as records of electronic transactions which are maintained by a shared or "distributed" network of participants (known as "nodes"), thereby forming a distributed validation system, that make extensive use of cryptography - that is computer-based encryption techniques such as public keys and private keys and hash functions, which are used to store assets and validate transactions on distributed ledgers.

This technology originated in the blockchain which a person or persons under the pseudonym "Satoshi Nakamoto" developed in about 2008 to create the peer-to-peer crypto-currency Bitcoin. In his paper on Bitcoin,[10] Nakamoto emphasised the attraction of a decentralised payment system by which electronic cash could be sent from one party to another without going through a financial institution or other trusted intermediary and which would make the payments

[9] Financial Markets Law Committee, "Fintech: issues of legal complexity" (June 2008) p 61; European Securities Markets Authority, "The Distributed Ledger Technology Applied to securities Markets" (7 February 2017), p 4.

[10] 'Satoshi Nakamoto, "Bitcoin: a Peer-to-Peer Electronic Cash System" (2008)

irreversible or at least impractical to reverse, thus removing the need for a merchant to trust his customer to pay for his goods or services.

This concept has undoubtedly appealed to anti-establishment libertarians. But Bitcoin has not been without its problems. As a permissionless system, it is open to the public, and members of the public can effect and verify changes to the ledger. But the method of maintaining the validity of the record on the ledger is extravagant in its energy use. The "proof of work" validation method used by Bitcoin involves the use of large quantities of computing power, as people "mine" to obtain further Bitcoins. It has been estimated that Bitcoin already uses as much electricity per year as the annual consumption of the Republic of Ireland (which has a population of 4.8 million) and that by 2020 it will consume as much as Denmark, which has a population of 5.7 million.[11]

Bitcoin has also proved to be the object of speculative bubbles. It has suffered crashes in value in 2011, 2013 and 2014, and particularly in 2017 when the coin rose from $1000 to over $19,000 before falling back sharply. When I gave a lecture on Fintech in Shanghai in October last year the price of a Bitcoin was about $6,400. When writing this lecture at the end of last month the price was about $3800. This price would be disappointing to someone who bought in when a Bitcoin fetched in the tens of thousands of dollars.

Other concerns about the crypto-currency have included the pseudonymous nature of the participants in its transactions. It appears to be attractive to criminals who wish to launder money and concerns have been expressed about its use in tax evasion, drug-trafficking and the funding of terrorism. Europol estimates that £3-4 billion is laundered using crypto-assets each year in Europe. While that is a small proportion of money laundering in Europe, a recent report by the Financial Action Task Force to the G 20 states that suspicious transaction reporting linked to crypto-assets is rising.[12] Digital currencies have also been used by the controllers of Ransomware, the malicious software used to prevent users from accessing their computer system unless a ransom is paid. While there may not have been breaches of the DLT ledger supporting

[11] The records of Bitcoin transactions are thought to be almost impossible to falsify because the collective computer power required to validate transactions is so great: World Bank Group, "Distributed Ledger technology (DLT) and Blockchain" (2017), p 6.

[12] Financial Conduct Authority, "Guidance on Cryptoassets" Consultation Report CP19/13, para 2.31.

the crypto-currency, there have been major problems with the software at Bitcoin exchanges at which the digital currency is exchanged for fiat currency. Thus, a Tokyo-based Bitcoin exchange, which had handled 70% of the world's Bitcoin trades, had to be closed down in 2014 after thefts of over $450 million worth of Bitcoin were discovered and in August 2016 $72 million worth of Bitcoin were stolen in a hack of the Bitfinex exchange. In the first 10 months of 2018, $927 million were stolen from coin exchanges by hacking, including $500 million from a hack on the Coincheck exchange.[13] More recently, it has been reported that the sudden death of the 30 year old founder of QuadrigaCX, Gerald Cotten, has left up to $190 million of crypto-currency beyond the reach of their owners as they were stored offline in "cold wallets" on his encrypted laptop and nobody knows how to get access to them.

The extent of fraud and serious misrepresentation in initial coin offerings (ICOs) has done much to discredit this means of unregulated funding. The Financial Conduct Authority has spoken of market volatility and the lack of transparency and oversight heightening the risk of market manipulation and insider dealing on exchanges and trading platforms and there are proposals to extend the regulatory reach of the FCA to bring in further types of crypto-assets and to apply anti-money laundering regulations to them.

I doubt whether the future lies with permissionless crypto-currencies with decentralised validation. But I expect that there remains a bright future for distributed ledger technology and probably also for digital currencies which are developed (and possibly underwritten) by mainstream financial institutions and central banks. Several central banks are exploring the introduction of DLT-based digital currencies issued by a central bank and backed by fiat currency,[14] and large international banks are examining the introduction of digital currencies backed by reserves of fiat currency. In February this year, J P Morgan announced that they had created and successfully tested a digital coin representing a fiat currency using a blockchain-based technology.[15] JP Morgan see the digital coin as a means of achieving instantaneous transfers of value, reducing their clients' counterparty and settlement risk and decreasing requirements to hold capital. They are currently seeking regulatory approval.

[13] FCA (footnote 12) para 2.28.

[14] World Bank Group "Distributed Ledger Technology (DLT) and Blockchain" (2017), p 34.

[15] J P Morgan Chase & Co website, announcement published on 14 February 2019. https://www.jpmorgan.com/global/news/digital-coin-payments

Distributed ledger technology offers many benefits. You can trace the ownership of assets on blockchain. If a trusted institution controls the ability to alter the blockchain, DLT can provide an accurate record of prior transactions without incurring great expense. DLT has the potential to reduce the costs of banking transactions and international trade by eliminating the need for the transmission and handling of paper documents and simplifying cross border payments. The FCA reports that there have been cases in the regulatory sandbox, which I will discuss shortly, which have demonstrated on a small scale that exchange tokens have made payment services, such as international money remittance, cheaper and faster.[16] There is the potential to speed up and reduce the costs of transaction by reducing or even eliminating intermediaries in financial transactions. The World Bank quotes an estimate that the financial sector alone could achieve savings in the range of $15-20 billion per year.[17]

An important part of the savings may result from the use of "smart contracts", which are contracts whose terms are recorded in a computer language and which are automatically executed by a computing system. At its simplest, the smart contract involves an instruction to the computer that if X happens then the computer is to act to make Y the result. In other words, the smart contract is performed automatically without human intervention. This removes or reduces the risk of default and avoids the cost of enforcement of contractual obligations. If you agree to transact by computer using smart contracts, you get automatic performance. It is like putting money into a vending machine to buy a bottle of water. The computer's "if-then" logic operates: money in, bottle out.

The reduced dependence on intermediaries, such as Central Counterparties (CCPs), and the reduced risk of default, which blockchain technology can offer, are seen as a means of improving financial market infrastructure. In a recent paper,[18] Professor Avgouleas and Professor Kiayias argue that the use of DLT systems in securities and derivatives trading, clearing and settlement has the potential to transform the structure of the financial services industry. The dependence

[16] FCA (footnote 13) para 3.54.

[17] World Bank Group (footnote 15) p 16.

[18] European Business Organization Law Review (2019) pp1-30, "The Promise of Blockchain Technology for Global Securities and Derivatives Markets: The New Financial Ecosystem and the 'Holy Grail' of Systemic Risk Containment." (28 February 2019). link.springer.com/content/pdf/10.1007%2Fs40804-019-00133-3.pdf

on and concentration of power in the hands of a few CCPs in derivatives trading is seen as giving rise to systemic risk and also creating moral hazard because a CCP may be too big to fail. In securities transactions, the costs of the use of investment intermediaries which hold securities as depositaries and the risks associated with the re-hypothecation of securities which have been received as collateral in one transaction, as collateral in a second transaction are seen as problems. The authors suggest that DLT systems can reduce that dependence on intermediaries, give the ultimate investor more control over the securities which it owns, and increase transparency and traceability. The new technology can reduce costs and, the authors suggest, create greater transparency and liquidity for long-term finance by creating markets for previously illiquid investments.

There is considerable international interest in the potential of DLT technology. Securities exchanges in Canada and Australia have declared their intention to move to blockchain operated trading and clearing and the South Korean capital markets regulator advocates collaboration in developing an integrated blockchain system for stock transactions. The Bank of England has been studying how a real time gross settlement service could be adapted to support settlement in systems using DLT technology. A consortium of Hong Kong and Singapore-based banks have started using DLT technology for processing trade finance documentation, following a successful trial which suggested that there were savings in time and cost from the use of the technology.

AI and the ability to process rapidly so much more data than was possible in the past should assist institutions to make better evidence-based decisions. Sophisticated investors and commercial organisations may be able to benefit greatly from what technology can offer, including in the area of peer-to-peer lending. But there are also important risks that ought not to be underestimated. The availability of big data and the ability of computers to process and analyse the data in ways which were previously not possible give rise to unprecedented ethical and regulatory questions. Since at least 2008 the ethical standards and responsibility of financial institutions have been the subject of adverse public debate. More recently, similar questions are being asked of the principal providers of technology such as Facebook and Google. In short, can financiers and big tech be trusted with the power which the information revolution gives them?

Concerns have been expressed about the potential for data to be used in unacceptable ways. Big data threatens privacy. The increased capacity to combine and process data from various sources has made it easier to identify individuals who are data subjects. Reidentification technology may undermine the current views of what is personal data. Algorithms could be used to restrict certain people's access to finance or insurance on unlawfully discriminatory grounds; they can be used as means of social control. The misuse or loss of data stored "in the Cloud" will be a concern if financial services are provided in this way;[19] cybersecurity is a challenge, for, while financial institutions constantly build their defences, cyber-criminals develop ever more sophisticated means of attack.

There may be a need to protect retail consumers from risky products by limiting access to certain platforms only to sophisticated investors. This may be the case with platform lending, as currently platform providers do not owe any form of a fiduciary duty to lenders in crowd funding should things go wrong, and things did go wrong in many ways in China where these platforms first claimed a substantial market share, forcing a government crackdown. But there may also be problems for financial institutions. 55% of trades in United States equity markets and 40% of such trades on European markets are automated with all key decisions made by algorithmic programs.[20] The Financial Stability Board ("the FSB") has warned of the danger of "herding" in financial markets. This is the process by which traders adopt similar machine-learning strategies and so amplify financial shocks. The FSB has also warned about the danger that insiders and cyber criminals may be able to manipulate market prices by identifying predictable patterns in the behaviour of automated trading strategies.[21]

Another concern which has been identified is the risk that financial markets may become too dependent on a limited number of technology suppliers so that the insolvency of, or other disruption to the business of a big supplier could disrupt the market.[22]

[19] Cheung and Weber (eds) "Privacy and Legal issues in Cloud Computing" (2016).

[20] Turner (fn 2) p 26.

[21] FSB papers, (i) Financial stability implications from FinTech: supervisory and regulatory issues that merit authorities' attention" (27 June 2017) and (ii) "Artificial intelligence and machine learning in financial services" (1 November 2017).

[22] FSB, paper 2 in footnote 13, p 33.

The development of Fintech also poses a challenge to the legal systems of the United Kingdom. We have long taken pride in having legal systems which promote commercial activity and which can be adapted to cope with changing circumstances. Lord Goff in an extrajudicial writing spoke of judges being there to give effect to the transactions of business people and not frustrate them; we, he said, "are there to oil the wheels of commerce, not to put a spanner in the works, or even grit in the oil".[23] Oiling the wheels of commerce when businesses are developing novel means of transacting though the use of AI and machine learning poses a serious challenge to lawyers, judges and legislators.

Much of the literature on the challenges posed by AI and machine learning has focussed on robotics, including the development of weapons and driverless cars. Perhaps the principal concern is the attribution of responsibility for the acts and omissions of robots. Only last week the Lord Chief Justice of England and Wales announced the establishment of an advisory body to offer guidance to the senior judiciary on AI and its impact, including its effect on the law. I hope that that body's work will extend to Fintech or will result in the creation of a body to examine the use of technology in financial practice.

Because of the importance of contract law in financial transactions, I will begin with that.

Contract law

Both English law and Scots law should not have much difficulty with questions about parties' intention to enter into contracts and the interpretation of the contracts because of the objective approach which we adopt. So long as the operation of the computer program can be explained to judges who, like me, may be deficient in our knowledge of computer science, it should be relatively straightforward to conclude that people who agree to use a program with smart contracts in their transactions have objectively agreed to the consequences of the operation of the "if-then" logic of the program. In the context of financial transactions, the English law

[23] Lord Goff of Chieveley, "Commercial contracts and the commercial court", [1984] LMCLQ 382, 391.

requirement for consideration should not be a serious difficulty and the flexible law of estoppel can, if needed, ride to the rescue.

The self-executing smart contract cannot be unscrambled in the same way as a traditional contract because it is not possible to annul it and halt its performance in the course of execution. The smart contract's strength in eliminating default by causing X to bring about Y, prevents the courts from stopping the performance of the contract. Rescission is not an option for the contracting party.[24] This means that the remedies for, say, fraud or misrepresentation inducing the contract are to order the re-transfer of property which has passed under the contract. This could be achieved by a declarator or declaration that the contract was induced by fraud or other misrepresentation and an order for re-transfer, by developing the law of unjust enrichment to reverse the effect of a contract which has not been rescinded.

Much greater problems in the law of contract may arise if computers are developed to use machine learning to optimise the transactions which they enter into. If businesses were to use computers with machine learning capability to deal with other computers with similar ability, they could autonomously generate transactions which would not fit easily into our contract law. Could one party to the contract turn to the other and say, like Aeneas to Dido, "non haec in federa veni", or "that wasn't the deal"? Or should the law say that those who willingly use computers with machine learning to effect their transactions are to be taken as intending to be contractually bound by the deals which those autonomous machines make? If a financial institution could walk away from a machine-created transaction, that might create chaos in the commercial world. If there is to be a contract drafted or adapted by machines, there will have to be significant development to our law of contract which will require careful and imaginative consideration.

It may sound rather fanciful that commercial organisations would allow computers autonomously to devise and enter into contracts with each other. But it may not be beyond the realm of possibility since there are commercial advantages in allowing computers to optimise trading deals. And there is always the risk of unintended consequences. There springs to mind

[24] Unscrambling an executed contract on blockchain is difficult to achieve, requiring one to go back in the chain to a point before the contract, creating a fork and re-creating the chain without the impugned transaction.

the public relations catastrophe of Microsoft's chatbot "Tay" which was meant to be programmed like an inoffensive teenage girl. "Tay" had to be decommissioned within 24 hours as various computer programmers discovered how to game the chatbot's algorithms to cause it to send offensive messages containing conspiracy theories and racist, neo-Nazi and sexualised content.[25] It seems to me that there is great merit in the concept of the regulatory sandbox, which I will discuss, as a means of testing innovative Fintech in a relatively safe environment.

It is sufficient at this stage to state that if Fintech is developed to use machine learning to optimise contractual transactions, there is a need for our commercial law to develop new concepts to address that phenomenon. Questions about the intention to enter into legal relations, to whom that intention is to be attributed and how the terms of a computer-generated contract are to be recorded to achieve legal validity and interpreted will require innovative thinking.

Delict/tort

The law of delict and tort will need to be revised to attribute liability for harm caused by machines exercising AI. Taking the most common form of delict, the law of negligence, how does one develop concepts akin to the neighbourhood principle in *Donoghue v Stevenson* and the carefully crafted rules by which judges have developed the common law to place boundaries on the involuntary obligations which the law imposes? Sadly, it is not just a matter of the reasonable bot on the San Francisco tramcar replacing the reasonable man on the Clapham omnibus – these are just legal abstractions.

Ulpian's three classical legal precepts - "to live honourably, to injure no one and to give everyone his due" - can provide a basis for the regulation and self-regulation of human activity. In the law of negligence, reasonable foresight and proximity – the neighbourhood principle - have fixed the boundaries of involuntary obligation in many contexts. But how do you impose liability and give compensation for the failure of a machine to comply with Ulpian's precepts - to injure no one and to give everyone his due? And when one addresses economic delicts, namely the intentional infliction of harm by unlawful means, inducing breach of contract or conspiracy, which require a mental element of an intention to cause harm, or the delict of fraud, in which the knowledge or

[25] "The Telegraph" 24 March 2016. Turner (footnote 2), p 131.

belief of the misrepresentor is relevant,[26] how do you impose liability for the harm caused by the autonomous acts of computers?

Where financial institutions choose to use AI in transactions with each other the participants in such transactions can regulate their relationship, including responsibility for the outcomes of AI, by contract. But when harm is caused to persons who are not parties to the contractual relationship, we enter the field of involuntary obligation, that is delict (tort) or liability imposed by statute, or unjustified enrichment.

Questions of the attribution of liability are arising in relation to driverless cars. There the principal concern is to have remedies for personal injury and damage to property caused by the vehicle. Part 1 of the Automated and Electric Vehicles Act 2018 imposes liability for third party personal injury or property damage caused by an automated vehicle driving itself on a road or other public place on the insurer of the vehicle or, if it is uninsured, on the owner.

Similar but more difficult questions will arise in relation to attribution of liability and causation in the context of transactions performed by Fintech. Is liability for harm caused by the decisions of the machine to be imposed on the producer of the machine on a product liability model? Or should the owner or organisation which operates the machine be answerable for such harm? More fundamentally, in a market system in which it is entirely legal to impose economic harm on a competitor if one trades within the boundaries of the law, how do you define what is an economic wrong resulting from the autonomous acts of machines? Having identified what is an economic wrong in such circumstances, should the law impose strict liability for the harm caused by the acts of machines or should liability be imposed on the natural or non-natural person producing, owning or operating the machine only if a natural person could reasonably have foreseen the risk of harm? These are fundamentally important questions of legal policy and the common law does not provide any ready-made answers.

[26] Joe Thomson, "Delictual Liability" (4th ed) chapter 2.

To my mind, a no-fault compensation scheme funded by a levy or taxation, such as is available in New Zealand to compensate personal injury, is a non-starter because of the potential scale of economic loss compared with the compensation paid under such a scheme for personal injuries.

There seems to me to be scope for a regime of compulsory third-party insurance which like that of the driverless vehicle could be on a no-fault basis, but there is a problem as to the amount of insurance cover which could sensibly be required. In the UK compulsory third-party motor insurance in respect of property damage has been fixed at the comparatively modest level of £1.2 million.[27] The potential scale of liability for economic loss from financial transactions is on a quite different level from liability for personal injury or physical damage to property. What would be a prudent and economically manageable level of compulsory insurance for Fintech and how many insurers will be prepared to offer such cover in the absence of product standardisation and a legal certification process?

These questions can be answered. But they need to be addressed.

Property law

There is also a need to adapt the law of property to cope with the assets which are the product of Fintech.

The Financial Conduct Authority does not view exchange tokens such as Bitcoins, Ether and Litecoin as money. While used as a means of exchange within digital communities, their volatility, which I have mentioned, militates against their use as a unit of account or a store of value. Fewer than 600 merchants in the United Kingdom accept exchange tokens as a payment tool.[28] The Financial Markets Law Committee has suggested that digital currencies which are pegged to fiat currencies could be regarded as "e-money" and be negotiable. The FMLC suggests that the traditional categories of English law could be extended to recognise virtual choses in possession as a new form of property.[29] In Scotland, where our property law has a

[27] Road Traffic Act 1988, section 145(4).
[28] FCA (footnote 12) paras 3.31 – 3.34.
[29] Financial Markets Law Committee, "Fintech: Issues of Legal Complexity" (June 2018), pp 30 and 38.

strong civilian framework we would need to recognise a new form of intangible moveable property.

A re-examination of the suitability of the tools of property law and trust law for our modern financial system would be a good idea in any event. There has been a debate for several years now on modernising, or at least clarifying, the law to accommodate intermediated securities. Intermediation at its simplest is the chain from the issuer of a security through the registered holder (such as a central securities depositary in the CREST system), via one or more intermediaries to the ultimate account holders. The question of the rights of the various parties in the chain and, in particular, the protection of the interest of the ultimate account holder has engaged the FMLC, the Law Commission, the UK Government and, in relation to private international law, international bodies for several years.[30] DLT is seen by some as a possible solution to some of the problems created by intermediation. A careful examination of this possibility together with an examination of appropriate legal rules for digital currencies and DLT transactions would be a major undertaking but, if successful, it would serve to provide a legal infrastructure to facilitate Fintech.

Another matter which needs to be addressed is whether the AI involved in Fintech should give rise to intellectual property which the law should recognise. If machines act autonomously to create new contracts, should there be copyright, and who should own it? Similar questions arise in relation to patents if such machines invent things which have industrial application. In relation to copyright, UK law treats as the author of a computer-generated work the person by whom the arrangements necessary for the creation of the work are undertaken.[31] This approach appears to have considerable potential to create disputes, particularly if a machine is involved in the arrangements.

Separate legal personality

One option for addressing the various questions arising out of the use of AI in Fintech is to explore whether to give a computer separate legal personality. While at first blush, that may

[30] Louise Gulliver and Jennifer Payne (eds), *"Intermediation and Beyond"* (2018), especially chapters 1, 3, 5 and 7.

[31] Copyright, Designs and Patents Act 1998, sections 9(3) and 178.

sound far-fetched, there is no reason in principle why the law cannot create such personality. English law has for a long time allowed an office occupied by a natural person to be a corporation sole, the separate legal personality of a "one-person" company has been recognised since 1897[32] and, more recently, in *Bumper Development Corporation*,[33] it has recognised the separate legal personality in Indian law of a ruined temple which was little more than a pile of stones.

It would be possible for the machine as a separate legal person to own intellectual property and in turn to be owned by a financial institution. That institution's licence or the general regulatory law could impose on the firm responsibility for any malfunction, if, for example, it had been involved in the design of the algorithm. The law could confer separate legal personality on the machine by registration and require it or its owner to have compulsory insurance to cover its liability to third parties in delict (tort) or restitution. And as a registered person the machine could own the intellectual property which it created.

How the law should be adapted

It will be clear from what I have said up till now that it is not practicable to develop the common law through case law to create a suitable legal regime for Fintech. The judiciary does not have the institutional competence to do so. The changes in the law which are required are not interstitial law the making of which is the long-recognised task of judges; they will require inter-disciplinary policy-making and consultation which a court cannot perform when resolving individual disputes and developing case law.

The Lord Chief Justice's initiative last week in setting up an advisory body is very welcome as a means of alerting the judiciary and the court system to the opportunities and challenges of AI. But a larger scale collaboration involving the executive branch of government, focussing on AI and Fintech and aiming to produce facilitating legislation is probably needed if the UK is to facilitate the development of Fintech without harming the integrity of the markets or financial

[32] *Salomon v A Salomon and Co Ltd* [1897] AC 22.

[33] *Bumper Development Corporation v Commissioner of Police of the Metropolis* [1991] 1 WLR 1362.

consumers. As the Law Society of England and Wales has stated (in a related context): "The statutory approach ensures that there is a framework in place that everyone can understand".[34]

International conventions and model laws

The United Kingdom's financial services industry is global in its reach. If Fintech is to achieve its potential and contribute to the economic welfare of this country and other countries, legal reform and regulatory change cannot be confined to the domestic market but must aspire to promote cross-border financial transactions and to facilitate international trade.

The current conflicting approaches to the treatment of cryptoassets by key jurisdictions such as the USA, the EU and the UK support the case for international cooperation in the creation of Fintech law.

One option would be to develop a model law along the lines of model laws which the UN Commission on International Trade Law (UNCITRAL) has developed and states have adopted. Another is the preparation of an international convention. At the very least there needs to be international cooperation to establish agreed rules of private international law to establish the governing law in relation to contracts executed and property held in a distributed ledger which operates across borders. I wonder if UNIDROIT, the International Institute for the Unification of Private Law, might have a role to play? It seems to me that the involvement of an intergovernmental body might reduce the suspicion by developing countries that large developed economies were dictating the rules. An alternative would be to build up a multilateral consensus between the leading trading nations.

Regulation and regulatory sandboxes

There is an increasing awareness outside the field of financial services of the risks that AI and big data analysis pose to privacy and human rights. Just as people can be excluded from flights and train stations, so also can Fintech be designed to promote social control and achieve social exclusion. It will all be in the algorithms.

[34] The Law Society's written evidence to the House of Commons Science and Technology Committee Report on *Robotics and artificial intelligence* (12 October 2016), quoted by Turner (footnote 2) p 223.

The preparation of statements of ethical standards has a role to play. But I doubt whether there is a public appetite for self-regulation in the financial services and tech industries. There needs to be regulation to protect investors and consumers, to promote market integrity and to preserve financial stability. At the same time, a regulatory regime must not stifle innovation. The FCA's invention in 2015 of the "regulatory sandbox" is to my mind a very important innovation. A regulatory sandbox is a framework set up by a financial services regulator to allow small-scale live testing of innovations by private firms (operating under a special exemption or limited temporary exception) under the supervision of the regulator.[35]

The sandbox allows the private firm to test products and services on a small scale with appropriate financial backing to indemnify consumers against loss and enables the regulator to assist in identifying safeguards to protect consumers which should be built into such products and services. This collaboration should enable them to be taken to market speedily.

Another possible use of a regulatory sandbox would be to analyse transactions to test the efficacy of proposed legal rules which could form a statutory framework of applicable rules on contract law, delict or tort, and property.

The regulatory sandbox has proved to be popular internationally and in August 2018 the FCA and eleven other regulators announced the creation of the "Global Financial Innovation Network". This is intended to create a so-called "global sandbox" which would enable firms to trial new products in several countries at the same time and allow regulators to exchange ideas on policy.

The international harmonisation of regulatory standards would serve to discourage financial institutions from seeking out jurisdictions with the least effective regulation as a base for their Fintech business. Discouraging such regulatory arbitrage ought over time to enhance market integrity and consumer protection.

[35] This definition is derived from Jenik, Ivo and Kate Lauer, "Regulatory Sandboxes and Financial Inclusion." (October 2017) Working Paper. Washington, DC: CGAP.

Conclusion

Financial services play a very important role in the economy of the United Kingdom, including the economy of Edinburgh. Our country has a great interest in establishing a leading position in the development of Fintech. An important precondition of establishing and maintaining the United Kingdom as a centre of excellence in the development and operation of Fintech is the development of our laws and regulatory systems to facilitate the use of such technology. This is a big undertaking. It requires a collaboration between financiers, computer specialists, judges, lawyers, law reform bodies and legislators.

Data is power, and AI is power. Can the law cope? My answer is yes, but it will require legislation. There also needs to be innovative regulation. Further, there is a need for international agreement on legal and regulatory norms if Fintech is to achieve its potential in wealth creation and poverty reduction through cross-border transactions while maintaining market integrity and protecting the consumer.

Thank you.