HOUSE OF LORDS

Revised transcript of evidence taken before

The Select Committee on Economic Affairs

Inquiry on

DISTRIBUTED LEDGER TECHNOLOGIES

Evidence Session No. 1 *Heard in Public* *Questions 1 - 18*

TUESDAY 19 JULY 2016

3.05 pm

Witnesses: Dr Ben Broadbent

Dr Catherine Mulligan, The Lord Spens and Professor Michael Mainelli

Mr Simon Taylor and Ms Blythe Masters

Members present

Lord Hollick (Chairman)
Lord Burns
Lord Darling of Roulanish
Lord Forsyth of Drumlean
Lord Kerr of Kinlochard
Lord Lamont of Lerwick
Lord Sharkey
Lord Tugendhat
Lord Turnbull

_____

Examination of Witness

Dr Ben Broadbent, Deputy Governor, Monetary Policy, Bank of England

Q1 The Chairman: Dr Broadbent, I welcome you to the Committee on this rather warm afternoon. If you feel like following our example and taking your jacket off, please feel free to do so. As you know, we are having a one-day hearing with three panels in it to gain a greater understanding of blockchain. It would be very helpful to hear from you what research the Bank is doing into blockchain. The Governor recently referred to it in a speech he was going to give at the Mansion House. He did not in fact give it, but it was published online, and it said that a research programme was under way.

Dr Ben Broadbent: Thank you for inviting me. In his speech, the Governor referred to so-called fintech in general. Perhaps the first thing to say is that that involves a lot more than just blockchain, or distributed ledger technology, and its implications for central banks, even if that is clearly one of the things that we are most interested in. There is a lot of other work that we are doing and are interested in beyond that as well. The Governor referred to some of that—analytics of big data, cybersecurity—in his speech, so it is not just the potential use of the blockchain.

The other thing to say up front is that this is a technology very much in its infancy, so its implications are far from clear at the moment. They are no clearer than the potential use of the internet was in, say, 1990. We view ourselves—indeed, I imagine the whole industry views itself—as being very much at the early stages of any research. I guess there are two broad parts of it. One is to think of the economics, particularly when it comes to the use of

the technology for payments or cryptocurrencies and things like that. The other is to follow closely what is going on, what the companies themselves are doing. That is one of the main reasons for the accelerator, so-called, that the Governor announced in his speech: to understand where things might go. Those are the two broad parts of what one might call our research programme.

The Chairman: You say that it is in its infancy. In your view is the prospect of a digital currency is some way off?

Dr Ben Broadbent: If by that one means an all-singing, all-dancing central bank digital currency not just replacing the liabilities that we currently have but prospectively substituting for commercial bank money, then yes, I would say so. It is not simply a question of the technology. Earlier this year, I gave a speech that was designed to say that this would also be a matter for the shape of the financial system. It is not simply technological barriers that one has to think about. As I said, that is really only one aspect of the technology. There are more immediate things, and we are, as it happens, undergoing a review of our own settlement system, the RTGS. That is necessary, not specifically to allow for any distributed ledger, but there are certain technical improvements that we need to make to it. We are undergoing a review at the moment. That review will be published early next year. As it happens, we want to think about what will be involved technically, at least, in placing central bank money on some distributed ledger. In my speech, I talked about a much more extreme version of that and whether, once you had done this, you would ever want to allow much more widespread access to the balance sheet of the central bank than what is currently enjoyed. I do not think that is under active consideration as part of the RTGS review.

The Chairman: If that were allowed, it would represent quite an existential threat to the existing banking system.

Dr Ben Broadbent: There are costs and benefits, but that extreme version at least would certainly have material consequences for the funding of banks as it stands at the moment. What I am saying is, one would have to think those through and not just whether it is technically possible to achieve something like that.

Lord Tugendhat: I find it very difficult to get my head around this subject. As you say, it is some way off and there are difficulties to overcome. It is therefore difficult, I imagine, to give a very clear answer to a question about what you think the benefits of a central bank digital currency might actually be and how widely they would be felt. Clearly everything will depend

on the extent to which the technical issues have been overcome. It may be that whatever benefits there are would come gradually rather than immediately. Do you feel able to say anything to enlighten me on that?

Dr Ben Broadbent: My feeling at least, which I tried to outline in the speech, is that conceptually—and accepting the fact that the technology may take us to different places and allow for different things—when it comes to the central bank, some of these questions are similar to those posed by what is called narrow banking. A narrow bank is one whose assets are as liquid as its liabilities. That is not the case for the banks that we have today and never really has been. Most assets of banks today are illiquid. They are loans whose value cannot be realised instantaneously, whereas many of their liabilities are deposits, most of which are on demand deposits, so you and I can go into a bank and transfer our money somewhere else immediately. That imposes a risk to the system and is why we have insurance in the form of lender of last resort, for example, or explicit insurance of deposits. That is also why we have vast amounts of regulation of the banking system. As it turned out in 2008, maybe there was not enough, or not enough of the right kind. The structural vulnerability of what is called fractional reserve banking, where the liquid assets are only a fraction of the balance sheet, is always there. A narrow bank is one that says that in order to have liquid liabilities, which people value as it is very nice to be able to hold deposits of a fixed value that you can move around instantaneously, it is obliged to hold equal amounts of very liquid assets such as reserves at the central bank or short-term government liabilities.

That debate about whether the banking system should or should not look like that goes back centuries. Indeed, it goes right back if not to the origins of the Bank of England then certainly early on, and to the Bank Charter Act in the middle of the 19th century. The great classical economist Ricardo argued that the note issue should be separated and backed only by liquid assets. The Bank of England was a private bank at that time. The debate is that, on the one hand, there might be added security in having a banking system that is not vulnerable to runs because it always has as many liquid assets as it has liabilities. On the other hand, there might be something intrinsically valuable about this so-called maturity transformation. There might be something economically necessary in having intermediaries who both issue deposits and do the illiquid lending. I was not, in the speech, trying to resolve that debate. Indeed, I pointed out that any very long-standing question by its nature will not be easy to answer. I was really saying that if one imagined a very extreme example of a digital currency

from the central bank, one that would gobble up and displace all these commercial bank deposits, we would end up with a particular kind of narrow banking structure. Essentially, you would have one enormous, nationalised narrow bank, and you and I would deposit at the central bank. We may hold some commercial bank deposits as well, but loans would then be funded in a rather different way, with more wholesale funding. As I say, the benefits of that might be that you end up with safer deposits.

On the potential costs, you would end up with costlier lending. In particular I was trying to get across what would happen if you wanted the co-existence of both those things. Suppose you wanted both existing at once so that you could hold a deposit directly at the central bank. It would be like a more useful version of physical cash. You would also hold a commercial bank deposit. Most of the time, you would feel that they were pretty close substitutes. You could transfer money between them and they would have the same value. At times of financial stress, when suddenly you began to trust your commercial bank deposit a little less, you would expect big transfers from one to the other. The particular thing that I was not worried about but trying to think about was whether that would be a good or bad thing. When you think of things on these scales, the benefits are clear and quite large, but so are the costs. I was really trying to say that even though this is a very new technology, once you think through it you realise that some of the very big questions involved are very old, not to say ancient—at least, ancient relative to the history of economics. They are there right at the start of the subject, really.

Q2 Lord Forsyth of Drumlean: I should declare an interest as a director and chairman designate of a bank. The private sector seems to have shown the most interest in adopting this technology for clearing and settlement purposes. Do you think these estimates of $16 billion of annual cost savings realistic?

Dr Ben Broadbent: This is where I must reiterate the fact that we are really at the start of this. My answer is: who knows? Frankly, in the grand scheme of things, when you compare it with the GDP of developed countries, it is a very small number. If this is an important technology, I would hope for savings that were rather bigger than that.

Lord Forsyth of Drumlean: Do you see the private sector coalescing around one distributive ledger for clearing and settlement, or is it more likely that several competing ones will develop?

Dr Ben Broadbent: There is a clear advantage with a lot of these technologies to having a single standard and platform. There are increasing returns to scale. It would be entirely typical and to be expected, not to say desirable, that for a period of time we will have competition between various alternatives. If we were to see the technology develop first in the clearing and settlement of securities or financial assets generally, I do not think there would necessarily be a unique ledger for everything, but we would end up with fewer than initially on offer. I think that is probably reasonable to expect.

Lord Forsyth of Drumlean: Last year, the Bank of England paper said, "It may be possible in the future—in theory, at least—for the existing infrastructure of the financial system to be gradually replaced by a variety of distributed systems". Is there enough processing capacity to process the world's entire payments and settlements system using this technology?

Dr Ben Broadbent: It rather depends on what that looks like. I am no technical expert; you have others far more qualified in that respect following me. I will say, however, that it has been noted before that the energy use involved in bitcoin is material. One important reason for that is because bitcoin is what is called a permissionless system. Anyone can join, anyone can transact and it is entirely anonymous. To verify transactions when you have absolutely no idea who people are—one of its virtues, of course—a lot of checking needs to be done. Proof of work is the particular method that that technology uses, which uses up a lot of energy. You can think of that as the price of trust, or the price of not having trust. In the absence of knowing who you are and what the business is—this is what the ledger can replace—you need a lot of verification of the transactions. The others who follow me will be able to tell you more about this, but my guess is that the systems we are talking about here are called permissioned systems, so that you do not operate on an anonymous basis. The participants in the ledger for clearing securities would, to one degree or another, be known by each other already. You would sacrifice some degree of anonymity, but you would also save in the costs of operating such a system.

Lord Forsyth of Drumlean: Do these savings that are being thrown about take account of the costs of the computer systems?

Dr Ben Broadbent: I would imagine so, but I emphasise again: my guess is that $16 billion is about what the OECD produces in total GDP every couple of hours, so these are not huge numbers. Given the investment in these firms, I would imagine that that is an entirely reasonable estimate. Certainly those investing in this space believe so.

Lord Forsyth of Drumlean: There is a bit of a track record of people expecting great savings from technology that then turns out to cost considerably more and return considerably less.

Dr Ben Broadbent: That is true, but there are other technologies where the returns have been much larger, as I said. If, for example, after the bursting of the tech bubble you had asked most people, they would have said that it was all ephemeral and overdone. Certainly the assets involved in internet technology at that time were clearly overvalued.

Lord Forsyth of Drumlean: So they had not recovered from the millennium bug.

Dr Ben Broadbent: I would make two points. First, on the uses and social value of the internet subsequently, I do not think that the assets were underestimated in terms of their reach, including in the financial sphere. One tends acceptably over long periods of time to neglect how much that is true in the payment space, regardless of something like DL. Twenty years ago—actually, more than that—when I started my working life, I would have to pay for things with cheques that took days to clear. Before I could make any other transaction I would have to queue up in a bank. I do not have to do any of that now. It is not evident to me that these are underestimates.

As regards the funding of these things, particularly when there are competing firms of which only a few will succeed, sometimes people overpay, but the bursting of the tech bubble, which was on a much larger scale than this, did not do great economic damage, because a lot of that funding was equity, not debt. I would make the same observation about what is going on with this technology. It is not credit that is funding a lot of this.

Q3 Lord Sharkey: I probably understand how verification works for bitcoin in terms of the proof-of-work concept, but when you talk about central bank digital currencies, how would verification take place? It could not be proof of work, because we do not have enough electricity. How would verification work for a central bank digital currency?

Dr Ben Broadbent: Again, I do not know. I would not want to anticipate technology. This question certainly involves a lot more than just the technological stuff. As I explained earlier, there some deep questions about the entire shape of the financial system involved with this. I will say only that this is not quite the same thing. In this, there would be one party whose identity did not need to be verified at all: namely, the central banks. Indeed, one thing that I said in my speech, and this is a high-level point, is that it is not obvious to me that the operational savings would be as big as for the possible platforms for exchanging securities. Fundamentally, that is precisely because central bank money is trusted. If you take at one

end this permissionless bitcoin system and the use of the energy involved to substitute for trust, I would place central banks, as the ultimate clearer and settler with the ultimate settlement asset, right at the other end. It is less evident to me that if you already have a trusted hub through which certain payments clear, there are huge operational savings to be made. You already have that trust. It is not the same as a bitcoin question.

Lord Sharkey: The *Staff Working Paper* this month by Barrdear and Kumhof estimates that if we had issuance of 30% of GDP in central bank digital currency it would permanently raise GDP by as much as 3%. That is surely a huge incentive to move in that direction.

Dr Ben Broadbent: That is a very interesting piece of work that points to various potential channels through which that is the case. There are some operational savings, but there are mainly two other things. One is that it rests partly on the idea that seigniorage, the revenue that the state obtains through issuing a liquid asset that people want, goes up a great deal and is a more efficient means of taxation than other forms of taxation, so it substitutes for less efficient forms of tax. The other is the idea of a kind of QE effect: that somehow if we enlarge the balance sheet of the central bank, it depresses the interest rate and the cost of funding economic activity. Whether those are on the scale of the estimates in that paper I do not know. Certainly if it relied solely on having masses of QE, we can do that right now, of course. Indeed, we have done. QE is not quite 30% of GDP, but I would imagine that it is about 20% at the moment. I think it would need more than just one aspect, and one has to refine those estimates. I pointed out earlier that it has pretty significant consequences for what we want the banking system to look like, and those are pretty big questions.

Lord Sharkey: Does it represent a new kind of tool for the Bank? I am thinking here of the zero lower bound problem. Given where we are with QE and interest rates, does this potentially give the Bank yet another weapon?

Dr Ben Broadbent: Zero lower bound arises fundamentally because of physical cash. There is out there for all of us an asset that we can hold that has a zero nominal return on it. That constraint is there, whether or not there is also a digital version of it. To break through the zero lower bound, it is not the existence of a digital version of cash that matters; it is the abolition of the physical version. That is ultimately what would have to have happen. If everyone had, as it were, an Oyster card and could essentially put something on that, and if it was exactly the same as physical cash, and everyone was perfectly happy with it and gradually migrated away from physical cash, perhaps subsequently getting rid of cash would

be easier. But it is the abolition of cash that matters, not the existence of some digital alternative.

From our perspective, we have no policy to do that. The Bank of England has a policy, which I think is the right one, of meeting the demand for cash as it arises. There are absolutely no plans to abolish it. If we look at the demand for cash—and this has arisen more from people who want to hold it as a store of value than for transactional purposes—we see that it has gone up quite a bit. It has gone up relative to GDP since we introduced inflation targeting, which I think means that people have more trust in the value of that physical currency. It has gone up another little leg even relative to GDP since the financial crisis, which may be because people have slightly less trust in their commercial bank deposits. All I am saying is that, conceptually, the existence of a digital currency would have some bearing on zero lower bound but only to the extent that it made one more prepared to abolish physical cash.

Q4 Lord Turnbull: Like Lord Tugendhat, I am having difficulty getting my head round this, and it goes right back to the word "currency". Is it an electronic version of a given currency, with the same exchange rate as the real version—in which case, it is really a medium of exchange settlement—or is it a currency in the sense of having an exchange rate? In the example you gave, if the attraction of holding bank deposits—for reason of risk perhaps—declined, people would move across into the central bank version of it. What changes here is the volume, not the price, so is "currency" really the right word?

Dr Ben Broadbent: Let me say a couple of things. First, the terminology gets a bit confusing. One reason for this is that there are things out there, such as bitcoin, that are separate units of account—if I can use those words. Sometimes when people talk about digital currencies, that is what they mean. It is not just the digital bit: by currency, they mean a different way of measuring price or value. I do not think that is what we are talking about here, and as I said in my speech I do not think that is a material threat to existing currencies. It is very hard for people to switch entirely to new ways of measuring value. Indeed, even though there are plenty of bitcoin transactions, there is an exchange rate with the dollar that is extremely variable. The price of bitcoin has been pretty volatile, and even if you pay for things in bitcoin you will find that the bitcoin price moves around to offset the currency, so what the retailer gets is a fixed amount of dollars. I do not think that is what we are talking about. When it comes to the difference between a commercial bank deposit and some putative,

theoretical central bank version, what I had in mind was not an exchange rate difference but a possible difference in the interest rate paid on them.

Barrdear and Kumhof's idea bears some resemblance to an idea long before people thought of distributed ledgers—or even the internet, frankly—by James Tobin back in the mid-1980s. His idea was that the central bank should offer people deposits. As I said, he did not have some DL in mind; he said that you could turn up at the post office and just bank directly at the central bank. But he said—and he was right—that if you were going to have both kinds of deposit you would need a spread in the interest paid on them. You would pay a lower rate, because it is more trusted, safer and backed entirely by liquid assets at the central bank, but they would be worth the same. If you went into a shop, it would be worth the same. If it said £10 on your commercial bank deposit, it would buy the same amount of stuff. That is important for anything to be considered.

Lord Turnbull: Would it not be easier to understand all this if we reserved the word "currency" for things that have an exchange rate and some other phrase—medium of exchange—for where the exchange rate is fixed but it has these other characteristics of different degrees of trust and interest rate?

Dr Ben Broadbent: You could call this central bank digital currency digital sterling, in the sense that it is not a physical thing, but it is an already defined unit of account.

Lord Turnbull: I think that would help people like me who are struggling.

Dr Ben Broadbent: I have struggled and am still struggling.

Lord Turnbull: All these things that we call currencies can then have a central bank version.

Dr Ben Broadbent: Exactly. I do not think there is anything conceptually difficult. It is a different means of payment. Potentially, there are very large consequences for other forms of sterling, but we are not talking about some new unit of account or anything like that.

Lord Turnbull: For the Bank of England, is this a tool that gives it better control or are you worried that it is, in effect, a way that the people you are trying to control and regulate can take their business off into darker realms that you find more difficult to track?

Dr Ben Broadbent: Let me get away from the central bank stuff for a moment, because it is highly theoretical and poses big questions of technology and regulation. Let us leave that to one side and talk about whether there are regulatory consequences of other developments. That is probably the most realistic one at any point over the next few years. We welcome the development of these technologies. Technological improvement is a good thing, including in

the financial sphere. I talked earlier about how much the landscape has changed over the last 25 years in making retail payments and doing retail banking. That has all been a good thing. As regulators, we are not interested in whether technology is necessarily risky. If I think of the systemic risk arising in the financial system as arising from some combination of leverage and lots of herding in positions, I can see no particular reason why this technology makes those worse. It might make certain operational risks better. But it could also, in some spaces, move some activity away from the regulated sphere into less observed places. We would want to monitor that. The Bank of England supervises clearing houses and if activity moved away from those we would want to follow it.

Lord Turnbull: The annunciator screen is showing a debate on the Investigatory Powers Bill. That is largely driven by technology allowing people to escape the supervision of the state and misuse their power. The state is trying to catch up. I suspect that you could find the same thing in this sphere.

Dr Ben Broadbent: Yes and no. My guess is that we will end up with "permissioned" systems and, when it comes to clearing securities, people who offer this technology and are engaged in it will want those. My guess is that long before we get to some widespread retail version of digital sterling—you are right that that term is more accurate—there might be a demand to have central bank money involved in these platforms for clearing securities. So people will want the central bank involved in this stuff. I do not know precisely what that Bill involves, but people have said that bitcoin—the true digital currency, the different unit of account—with its entirely anonymous, permissionless system, can be favoured by people who are interested in escaping the scrutiny of the state, whether it is tax collectors or the police. I do not think that is what we would be most worried about. I think people would want us to be involved. When it comes to anonymity, and the costs and benefits of that, the state has faced that for centuries with the use of cash, which is probably used disproportionately more than observable high street bank accounts. There are still trade-offs involved there.

The Chairman: We have time for one more question in this session.

Q5 Lord Burns: I declare my interest as I remain an adviser to the Santander group. I would like to follow up a little more on the question of regulation, mentioned by Lord Turnbull, and what you see as both the prudential and conduct challenges of moving to this world. So far, you have described the first step of all of this which one might describe as back-office functions being affected. These are basically methods. Some of the deeper policy issues of

applying it to the currency are another step. Is it not inevitable that, as you move towards more distributed technology, the job of the regulators becomes more difficult? Anything that is peer to peer is going to be much more of a problem to monitor, from both a prudential and conduct point of view, than if you have large institutions that can be looked at in detail over a period of time and that catch one end of the transaction. Are we not already seeing quite interesting issues of conduct emerging in some peer-to-peer lending, where people do not have the guarantees they thought they had about what might be delivered?

Dr Ben Broadbent: I think that is true. In the retail space you would always be interested in whether people understand what they are getting involved in. From a supervisory perspective there are different aspects. If I can use prudential supervision. Some parts of this might make the system more robust. The thing about a distributed ledger, which is a problem for some of them in some ways, is that the information is shared everywhere. There is no transaction in bitcoin that is not known, or knowable, by every member of it—

Lord Burns: That is a strength?

Dr Ben Broadbent: I think so. It is a strength in terms of operational failure. It can be a weakness for us. Let us suppose that we had central bank money on some ledger and other banks were involved in this; it would make ELA lending potentially problematic for the central bank.

Lord Burns: So those sorts of initiatives where you have wanted to keep it under the counter purposefully.

Dr Ben Broadbent: Indeed. It is not necessarily the case that this technology leads to more things being hidden. If you are part of it, in principle you see everything—that itself may be an issue. From a conduct perspective, I agree that potentially there are things that one would keep an eye on, particularly in the retail space.

Lord Burns: Could I just follow up with another question on this issue of narrow banking that you raised at the beginning? You began to describe what it does to other forms of activity in which the banks currently engage. If I interpreted it rightly, it would mean that, when it came to mortgages, they would have to be done on a completely different basis—banks would no longer provide mortgages.

Dr Ben Broadbent: I do not think that I am saying anything new here. I imagine—I was not on the committee and it was not in the report—that the Vickers commission thought about

things like this. As I say, economists have been thinking about them, unfortunately with no clear conclusion, for the best part of a couple of hundred years. But, yes, a narrow bank is one in which the stickier lending would have to be financed with different kinds of vehicles and deposits. It might be equity; it might be wholesale debt, but it would be of a different nature from something that has a fixed value that you could take out of the institution at any time. At the margin at least, that would be true.

Lord Forsyth of Drumlean: Perhaps I do not understand this, but, picking up the point made by Lord Burns and Lord Turnbull about security and knowing what is going on in the system. You said that, with bitcoin, everybody knew the transaction. Is not the point that they do not know who has paid the money and to whom they have paid it?

Dr Ben Broadbent: They do not know the identity. They do not know the name or the rank, but they know the serial number. They know that this person who has done this transaction has now done this. There is nothing known to any member that is not known to all of them. So you are right to say that it is anonymous—

Lord Forsyth of Drumlean: So if you have someone transferring money to some terrorist or some drug baron around the world, does it not represent a risk whereby you know that money is being transferred, but you do not know why or to whom?

Dr Ben Broadbent: That is absolutely true.

Lord Forsyth of Drumlean: Is that not a huge risk?

Dr Ben Broadbent: That is true. Indeed, operationally, we would want to know more. If everyone can bank with us, we will want to know a great deal more about our customer, just as any commercial bank is obliged to know about its depositors.

Lord Forsyth of Drumlean: Perhaps I am seeing dragons where they do not exist. I guess that the people whom we have been concerned about in this context are not people who would want to bank with you. The question is: is this opening up a technology that will allow—

Dr Ben Broadbent: Let me come back to what I said. We are not opening anything up. We are in a monitoring phase and thinking about some of the questions involved—those are some of them. Conceptually, it would not resemble that. The uses of a distributed ledger in clearing securities would be fundamentally different in that they would be permissioned.

Lord Forsyth of Drumlean: But does bitcoin not provide for that? What am I missing here?

Dr Ben Broadbent: Bitcoin does, but it has huge deficiencies as a currency. If you think of what the definition of money is meant to be—

Lord Forsyth of Drumlean: My question is not about that; it is about risks to the system and to our security arising from the development of this technology.

Dr Ben Broadbent: They are potentially there. My answer was that bitcoin is not the right parallel, because I cannot imagine that we would use what are called permissionless systems. They are fundamentally different in that respect. If ever we did something like that—whether it was much more limited use, which I think is the more realistic version for clearing securities—we would never have a system like that. Indeed, the private sector itself, even left to its own devices and with no involvement of the central bank, is not thinking of systems like that as far as I am aware.

The Chairman: Dr Broadbent, thank you very much. That was very helpful.

Examination of Witnesses

Dr Catherine Mulligan, Associate Director, Imperial College Centre for Cryptocurrency Research, Imperial College London, **Lord Spens**, Transformation and Assurance Director, PricewaterhouseCoopers LLP, and **Professor Michael Mainelli**, Emeritus Mercers' School Memorial Professor of Commerce, Gresham College

Q6 The Chairman: Professor Mainelli, Dr Mulligan and Lord Spens, welcome to the Economic Affairs Committee. As you know, we are having a one-day hearing into blockchain to try to educate ourselves and, hopefully, others as well. We are on a fairly tight schedule, so if one of you responds to our questions and the other two agree, it is probably not necessary to do anything other than nod, but please feel free to speak if you disagree or want to elucidate a point. I have a general question to start with. Which industries do you anticipate blockchain having the most impact on? How disruptive, in particular in the financial sector, do you think it will be?

Professor Michael Mainelli: The interesting thing about this technology is that it is about diminishing the role of natural monopolies that are formed by central third parties, so I would expect the industries that are most affected to be those that have been hampered by an inability to form an organisation at the centre for efficiency's sake that hitherto would have abused its natural monopoly position. That leads to a host of areas: electricity transmission, insurance—particularly wholesale insurance—shipping, the entire nature of the sharing economy, health, media and identity systems. Those would all be areas where

we have typically had troubles forming some form of central third party and we have feared it, because in effect this technology moves two of at least three functions of a central third party into the technology itself—the preservation of the record, where everybody has a copy and it is immutable. It is distributed across multiple machines, so it is secure and reliable. But that leaves the question that you struggled with earlier with Dr Broadbent: what is the validation procedure that is used at the tail end? That is the important thing that we need to address, and where the variety is in the system, not in the blockchains themselves.

Dr Catherine Mulligan: I would probably agree and would add that government is another industry that would be broadly affected by this technology, as well as local authorities.

The Lord Spens: I would add airlines and the travel industry. They have to share data and it is a natural home for someone who has to share data.

The Chairman: How would you summarise the disruptive consequences of this in the financial services?

The Lord Spens: Santander looked into it and produced a report mentioning $16 billion. It is about stripping out inefficiencies in the back office.

The Chairman: That will lead to a substantial reduction in the number of people who are needed to operate financial services companies.

The Lord Spens: Depending on the speed of adoption and the evolution of the technology, potentially, yes.

The Chairman: On that question of speed, what stands in the way? Dr Broadbent said that we were at the infancy of this. What stands in the way of rapid rollout?

The Lord Spens: For the financial services specifically, it is collaboration. Banks do not need to share information. If you are an airline, a travel agent, you must share information.

The Chairman: I see; so that is an essential ingredient to rapid rollout.

The Lord Spens: Yes.

Q7 Lord Darling of Roulanish: First, I declare an interest as a director of Morgan Stanley. Professor, you started off by saying that one of the advantages was disrupting natural or otherwise monopolies, and you mentioned shipping and so on. Could you just explain what you mean by that?

Professor Michael Mainelli: There are a number of areas in the commercial markets where people have tried to set up central third parties. I would pick on, for example, Bolero in the shipping industry in the mid-1990s, the ACORD system and various failures of Lloyd's to

agree on a central market that clears. When people get into a position where they can hold on to all the data, they abuse those types of monopoly. We have seen this in the capital markets. Take, for example, the mutualisation and demutualisation cycles of the major exchanges. Until about 2000, the exchanges were mutuals and we shared the information. They were then effectively privatised or sold off. At that point, people were saying, "I actually own all this data and I am here to make money out of it. It doesn't matter what the numbers are". Then we saw the formation of Turquoise and BOAT, which were trying to form mutuals again, and so on. Societies have often struggled with this. Ultimately the technology is boring and it ought to be; it is about ledgers. The only excitement that we had with ledgers was when this place burned down in 1834 because of all the tally sticks. We are seeing a move to a new form of ledger technology. It has a lot of advantages, but the real effects will be on the economic and power structures of central third parties.

Lord Darling of Roulanish: This is where I am struggling a bit. Dr Broadbent, in his evidence to us just now, said that one of the advantages of blockchain would be that it would make performing clearing functions, for example, easier, more efficient, more effective and more transparent. He also said that, separate to that, you could facilitate technologies such as bitcoin and so on. You seem to be referring to creating something more like what the internet did—in other words, ultimately, making all information completely public. Is that right?

Professor Michael Mainelli: Not necessarily. A whole variety of things can be built with these ledgers, from the frankly absolutely opaque to the completely transparent—it is up to you and the settings that you put in. You can have documents that are completely encrypted, so that I know there is a document there, but I cannot look at it, or I can have an open document. There is a huge variety of blockchain technologies out there.

Lord Darling of Roulanish: Sorry, can you give an example of who would have information under this that they do not have today?

Professor Michael Mainelli: Let us take an identity system. I know that one of your questions was about Estonia. In the case of an identity system, I can put records on to the blockchain, but I can then have a key structure that gives me the ability to say, for example, "Lord Darling, you can see my passport and my driver's licence for a limited period of time and a limited number of looks. I pass that over to you." You will now open that using those keys.

The data itself is encrypted. Everyone else has access to the same data, but they are not able to see within it.

Lord Darling of Roulanish: So the whole world can look at your driving licence on five occasions.

Professor Michael Mainelli: If I gave the whole world permission.

Lord Darling of Roulanish: Why would you want to do that?

Professor Michael Mainelli: That is according to the sort of settings that you want. In Estonia, there are very strict controls on people's access to the data and they try to give the user control over it.

Lord Darling of Roulanish: What about my health records? As you know, Governments in different parts of the country wanted to use that information for general research, but that has been highly controversial. Is the idea that our health records could be up for grabs for someone to have a look at them?

Professor Michael Mainelli: Perhaps it could work more like this: perhaps it could be that you in fact control your own health records during your life and you surrender them on death because you would like to encourage further research.

Lord Darling of Roulanish: But I can do that now.

Professor Michael Mainelli: You can do that now as well. It is up to you. It is your decision.

Lord Darling of Roulanish: It would be very helpful to the Committee if you could give three examples of where we would be better off by having this technology than we are today. What three things could be done and are likely to be done in the not-too-distant future rather than in 100 years' time?

Professor Michael Mainelli: Let me quickly tell you a story. Last summer, we were approached by a group of US insurers. They were examining how they could offer differential electricity insurance, which means that you are allowed to turn on and off your appliances to do a little balancing so that you can get a lower electricity bill. The electricity company is deciding whether it will turn it on or off. You come home one day in Kansas, you open the freezer up and it is all mush—they have large freezers in America, so it is $4,000-worth of mush. You ring your home and contents provider, who tells you that you are not covered, because you have one of these new-fangled electricity policies and the company turned it off. You ring the company and it says that it was misinstalled by the freezer company. You ring the freezer company, which says that it was perfectly installed and you

might have unplugged it to hoover—or vacuum, as they say over there. You may have done that. In America, it is a line item in insurance and people claim at the end of the month rather than hitting the payday lenders, so they decide that they will open the freezer, let it melt and claim—they want to turn frozen foods into liquid assets. You have a whole situation there. How will you record that, because all those were micro-second by micro-second ledger entries? That is an area where these types of ledgers are there. IBM and Samsung have launched something called ADEPT, for the internet of things. I believe that they foresee billions of ledgers—autonomous vehicles, your home heating system, your home security system, your entertainment system and your phone. We need ledgers for all these things if we are going to live in a highly automated world.

Dr Catherine Mulligan: Could I clarify one thing about the data? The data is never actually stored in the ledger. What is stored is the transaction. The data is generally kept separate.

Lord Darling of Roulanish: So what is the transaction in health?

Dr Catherine Mulligan: The transaction in health may be a patient's journey through a hospital. For example, a paramedic coming through will automatically record all your data and put it ready for you at the hospital. The hospital follows the tracks of those transactions. A distributed ledger or similar technology is not necessarily about the data; it is about an internet of value exchange. It is about value, rather than data. There is a bit of a difference there.

The Lord Spens: You might have a situation where you have had an operation and your surgeon wants to track your progress, so you allow him to see copies of your pharmaceutical purchases. But you as a patient probably do not want your mother seeing that, so you just do not permission your mother.

Lord Sharkey: I may not have understood this, but on the data being captured but not the transaction, how can that be the case? I mean, it is data that we are talking about here.

Professor Michael Mainelli: May I beg to differ? There are numerous ledgers out there that hold the data directly. That is also a choice. Dr Mulligan is correct that you can build ledgers that do not store data, but you can build ledgers which do. The technique used to store a copy of the data entity, or a signature of it, is called hashing, so the ledgers that she refers to store only a hash of the data and the data is presumed to be elsewhere. We can then validate that the data ledgered was for the transaction by hashing it again and seeing whether we have the same signature. However, there are ledgers—I have some in my

pocket—that have been built to store the data directly themselves. It is a choice. There are a lot of design choices here.

Lord Darling of Roulanish: I am confused, Lord Spens. If I have an operation, I go to the chemist umpteen times. The surgeon is interested in what I was buying in the chemist's rather than the fact that I went to the chemist. That must be data on what I bought or had prescribed or whatever it was.

The Lord Spens: You can set up your blockchain-enabled solution for whatever business process it is and you can admission the one person.

Lord Darling of Roulanish: So blockchain to you is basically a system whereby you can disclose as much or as little as you want about what you are up to, which may be of benefit to a third party you have nominated but nobody else can get into it.

The Lord Spens: Correct. Blockchain is industry agnostic and it just replaces business process.

The Chairman: This requires the individual or the organisation to establish the rules, so you have a responsibility to do that.

The Lord Spens: Correct. Whatever the closed user group is, be it the London Stock Exchange or the hospital supply chain, you set the rules.

Dr Catherine Mulligan: That is why you need industrial collaboration.

Lord Darling of Roulanish: I understand that the DWP looked at this to track where people in receipt of benefits spent their money or what they spent it on. Did they know that that was happening?

The Lord Spens: I should declare an interest here. I am on the advisory board of a company called GovCoin Systems, which has a current proof-of-concept with the Department for Work and Pensions distributing benefits to south Manchester claimants today.

Lord Darling of Roulanish: Yes. Well, is my understanding correct?

The Lord Spens: A person in the audience is from DWP. Is he allowed to answer the question?

Lord Darling of Roulanish: No, you answer the question. He can tell you the answer, but if you could repeat it to me, it would be very helpful—if only because he does not have a microphone and I cannot hear what he is saying.

The Lord Spens: Can you repeat the question, then, please?

Lord Darling of Roulanish: My understanding is that, as an experiment or a trial, the DWP has been looking at technology that might help it identify in respect of someone receiving benefit where they were spending their money and on what goods and so on.

The Lord Spens: That is perfectly possible, but I am not sure that it is what the DWP and GovCoin are doing.

Lord Darling of Roulanish: So you do not know whether that is happening.

The Lord Spens: I do not know whether that is in the proof-of-concept.

Lord Darling of Roulanish: That example raises an ethical issue as to whether the state should know that someone is choosing to spend their money on one thing or the other.

The Lord Spens: I agree.

The Chairman: Would it not follow from your previous answer that the beneficiary would be able to exclude the DWP from looking at how it is spending its money?

The Lord Spens: Pre-paid cards have been around in South America for 40 years. They restrict where you can spend your money. It is how lots of people get paid.

Lord Darling of Roulanish: We do not live in South America.

The Lord Spens: I am saying that it is Parliament's choice.

Q8 Lord Kerr of Kinlochard: I should declare an interest as a director of an investment company. I think I detected that Professor Mainelli wanted to be asked about Estonia, so I comply and ask him about the Estonia experience: how well has the technology worked and what uses have the Estonian Government made of it? Can I ask a second question? If you think about how this is likely to develop and about the example of social media, it seems likely to me that we will be pretty rapidly back in the area of a monopoly. There will be a period in which various distributed ledger networks will compete. There will be a winner, and that will probably happen quite quickly. Is that correct?

Professor Michael Mainelli: The Estonian experiment began after the attacks by the Russians in 2007 on its cyber infrastructure. The Estonians decided at this point that they would like to adopt a blockchain-like technology both for the storage and the recording of documents, accesses and transactions. It runs on two systems: a PIN number and an electronic signature. The system appears to have worked quite well; it has been rolled out to 1.3 million residents in Estonia. The residents seem to like it, and it has been performing for some time. It has replaced effectively the bank identity system, because once I have identified myself to my ATM, why do I need a bank card to do it? I am that person who owns

that ledger in the bank. It seems to have been a great success. There are certainly attractions in considering this or something like it in the United Kingdom, for several reasons: first, the large cost of KYC-AML—know your customer and anti-money laundering—sanctions, screening and ultimate beneficial ownership; and, secondly, we have an immigration issue and this would be an address on it—of course, it would re-open that third rail of the identity card problems we had a dozen years ago. In answer to your second question on monopolies, this is something I think one always has to fear. As somebody who has been on the internet since 1976, I came with great visions of serendipity and a wonderful world out there, and now I look at these walled gardens. I share those concerns. There are some structural ways in which this might be different, but I am not wholly assured that we would not wind up creating a very large monopoly.

Lord Forsyth of Drumlean: Perhaps I am being thick here, but I want to pick on the point which Lord Darling made about social security and people's expenditure being tracked. Is that expenditure on a particular credit card? How is it tracked? How do they know what you have spent?

Dr Catherine Mulligan: It is on a mobile device. GovCoin is implemented on your mobile phone, so you will get an app.

Lord Forsyth of Drumlean: And you are required to use that phone for all transactions? So if you go down to the bookmaker and put something on the 2.45 at Newmarket, is that tracked?

Dr Catherine Mulligan: To clarify, I am not associated with that proof-of-concept, but my understanding is that the benefits cash would be paid into that. If you wish to spend your benefits, you would have to use that application.

Lord Darling of Roulanish: Could you take money off your app, put into your account at the NatWest and then go down to the bookies?

The Lord Spens: Yes, probably. You can set the rules.

Dr Catherine Mulligan: When I have read about this proof-of-concept, it seems that recipients can opt in to be able to say: "I would want to make sure that my benefit money was not spent on alcohol, drugs or gambling". So it is an opt-in system.

Lord Forsyth of Drumlean: But this is Big Brother writ large, is it not?

Dr Catherine Mulligan: Yes. An important thing about this technology is that it genuinely challenges us to think deeply about the sort of economy and society we want. There are a number of profound issues that we need to think about from a regulatory perspective.

The Lord Spens: So Big Brother potentially looms large and bad things can happen, but if we think about United Nations sustainable goal 16.9, we see that 1.5 billion people in the world do not have a legal identity. Without a legal identity, you cannot have any financial inclusion, education or healthcare. Human trafficking is now the third most profitable criminal activity in the world. Blockchain as a technology might help digital legal identity, much as it has in Estonian, and allow those 1.5 billion people into society.

Lord Kerr of Kinlochard: Can I come back to the brief Darwinian period and the emergence of a monopoly? You heard Dr Broadbent telling us that at the Bank of England it would be welcomed on the scene. That seems to be in conflict with what we are thinking about now, if it is the emergence of a monopoly. How will the regulator operate 10 years ahead if distributed ledger technology develops as we think it will?

The Lord Spens: I spent the last six years working for the regulator. I cannot speak for it now; I no longer work for it. But no regulator wants to regulate technology. What it would want to think about is your digital legal identity—and regulate that. In any closed user group, you need some form of identification to get in, an authentication. When you transact, you have verification of the transaction but you need identity to get in. If we give everyone a legal, digital identity on the blockchain, actually that reverses the internet.

Lord Kerr of Kinlochard: Surely what matters to the regulator is the volume of transactions. The policeman might be interested in the identity but the regulator is more interested in the volume.

The Lord Spens: Correct, so in order to get into the club the identity piece has to be proved. Once the transactions happen, you could have the regulator being sent a copy of every transaction.

Q9 Lord Burns: Earlier, we discussed with Dr Broadbent that a lot of the potential cost savings come through back-office functions. I am interested to hear, particularly in relation to your suggestion that this could apply to government and local authorities, the types of exercise this might be. What would the consequences be and where would the cost savings come from? What would that look like on the ground?

Dr Catherine Mulligan: Okay, so I will take a very simple example. At universities, we are often called and asked to prove or confirm that someone has the degree and grade that they say they have. That takes a lot of time and effort. The potential employer needs to pay an agency to do that, usually about £80, and it takes up to two to three weeks to get that answer. You need someone on the phone to go down to the archives, get the paper, copy it and say, "Yes, this person has that". Using a distributive ledger, you could build a system whereby the student would enable an employer to access a transaction on the blockchain or distributed ledger to say, yes, the university immediately confirms that you have a first-class honours degree in engineering from Imperial, for example, or from the University of Nottingham or somewhere similar. So that could remove a lot of time and cost.

Lord Burns: So the aim here would be to have all students on this system from all universities?

Dr Catherine Mulligan: Absolutely.

Lord Burns: And then an individual student would authorise the particular employer that they chose to look at this for some limited period of time.

Dr Catherine Mulligan: Absolutely.

Lord Sharkey: Would that not be the same with health records? With health records held in a distributed fashion, access would be given only with the patient's permission.

Dr Catherine Mulligan: It could be very similar. The only difference is that a university holds the student's entire record but in a healthcare record it may be multiple different entities: your GP, a hospital or a specialist.

Lord Sharkey: But that is a trivial fix, is it not?

Dr Catherine Mulligan: In theory, it is trivial, yes.

Lord Burns: But presumably, in this distributive ledger it would be possible to aggregate all the information about an individual.

Dr Catherine Mulligan: In theory, yes.

Lord Burns: On an anonymised basis. But then, on when you give permission, say you have an accident and are taken to hospital; presumably, the hospital could then ask for permission to see your whole-life medical record to judge whether the treatment it gives you is appropriate.

Dr Catherine Mulligan: Or if you have allergies or something.

The Lord Spens: You could have a situation where there is a two-tier insurance system. Someone who does not want to share their health records with their insurance company pays one fixed price. Someone who does share their health records on an ongoing basis, so that the insurance company gets real-time clarity about their health, might pay a lower premium. There will be multiple models and thousands of blockchains, not one big one.

Lord Forsyth of Drumlean: With insurance you are dealing with a pool and people benefit from that pool. Okay, some people with good health that is being monitored on a real-time basis may benefit. What about the problem that creates for people who do not have that? You lose the pool effect.

The Lord Spens: That may be true. I am not an insurance expert.

Lord Forsyth of Drumlean: But you would be selling it as an advantage.

The Lord Spens: There would be other providers.

Lord Burns: My final question: which industries, activities and types of firm will be most under threat as a result of these developments?

The Lord Spens: I would say that blockchain does four things. It removes the requirement for reconciliation, so it will affect anything with a large back-office. It removes the need for a middle person. If you do not want to use a middle person, you do not have to—so, that is insurance brokers, travel agents, stockbrokers and things like that. It provides immutable proof of provenance, so there is the Land Registry and things like that. You can embed business logic: if this happens, then that must happen. The combination of all that makes the technology very powerful. So it will affect any industry that has any combination of that.

Dr Catherine Mulligan: I was going to say, to turn your question on its head, one of the biggest opportunities is in local authorities for reduction of cost. They deal with so many disparate shareholders across their activities.

The Lord Spens: I agree. Government could become much more efficient across a number of departments.

Lord Burns: For local authorities, you are talking about things like planning applications—

The Lord Spens: Hospital supply chains.

Lord Burns:—and whether street lights are working, and all the services.

Dr Catherine Mulligan: Waste management, those kinds of things, yes.

Professor Michael Mainelli: So much of this is dependent on documentation. The Government Office for Science report in January said that something like 57% of all litigation

that costs us money in the Ministry of Justice is due to contract disputes. Again, just being able to say, "This is exactly what was agreed at that time" would lead to a large degree of cost saving, as it has started to already.

Lord Burns: That is just a question of whether or not you have done the paperwork properly at the beginning, as it were, and that it is recorded correctly. It is what the contract is that has been arranged. It does not need to be in a blockchain to get that. You cannot invent something that is not there. If people have not written it out properly in the first place, it will not suddenly come magically as the result of the interaction of these blocks.

Professor Michael Mainelli: There are many areas of complex commerce within the Lloyd's market. There are about 100,000 bindings every year. When these come to claims, huge amounts are paid to lawyers to figure out what was the situation at the time. Who saw what? What was the messaging on this? What was the certainty of the contract? What was included? Did I actually show you that video? Did I show you the video that I claimed to show you or did I show you another video? Believe it or not, these are huge areas of substantial cost.

Lord Darling of Roulanish: Most contracts are about interpreting words. I cannot see how launching this helps. It is not an automatic judging service, is it?

Professor Michael Mainelli: I am looking at bindings rather than contracts. The point here is that an insurance contract is not dependent on asymmetry of information, as a traded market is. It is about everybody sharing the information at the time in a spirit of goodwill. When the dispute arises, it transpires frequently that people have or have not shown certain things that they claim to have shown or looked at. This is why insurance markets in the United Kingdom have had substantial difficulties. This is a substantial section of GDP, and some estimates are a few billion off the cost of insurance within just the London markets themselves.

Lord Burns: Is it that in many of these cases, the answers are contained in strings of emails? There is the question of whether this video was shown or not, so you go through a whole search process. What you are saying is that, rather than being lost in some quagmire of emails, when each individual action took place it will have been explicitly entered into a ledger.

Professor Michael Mainelli: Correct.

Lord Turnbull: In the old days, if you wanted to re-licence your car, you got a letter saying it needed to be re-licenced. You went to the post office, but not before the end of the two weeks in which they gave you. You took along the piece of paper saying that you owned the car, an insurance certificate, an MOT certificate and a means of payment. Now, it all just happens. Is that a piece of blockchain technology or is it something else?

The Lord Spens: It is possible.

Dr Catherine Mulligan: Yes.

Lord Turnbull: It happens now. But would you call that an early triumph of blockchain technology or is it something else?

The Lord Spens: It is the fourth bit. It is the business logic you are embedding: if this happens and this happens, and this MOT certificate is valid, then take the money and give them the licence.

Lord Turnbull: They do not even give you the licence these days. They just say, "You are licenced".

The Lord Spens: That is the identification piece. You would have to go to the DVLA to start with and prove who you are, so that it could then be confident to enter into that contract—that if this happens, then that happens.

Lord Forsyth of Drumlean: The problem is that because you do not any longer have a licence, you do not know when your licence has run out. You end up being in default.

Lord Burns: They write to you.

The Lord Spens: You could go back to the business logic and send out a letter at the end of it.

Lord Turnbull: The thing I am worried about is that in order to conduct a very simple transaction, where you go on to the internet and all you want to do is buy a garden spade or something, you have to answer a whole questionnaire. It is very difficult to just do something simply. If I have to say, "Who am I? Who can see this and in what circumstances?" and so on, is that not going to slow things down rather than speed them up?

The Lord Spens: The blockchain is not the panacea for this; it will not cure everything in the world. There will still be a cash market. They will still be able to do normal transactions. If you want to buy a garden spade, I would recommend not using blockchain.

Lord Turnbull: You talk about blockchain technology. In a lot of cases, there are different technologies. People had different models, such as VHS and Betamax, or the Stephenson

gauge versus the Brunel gauge, and they slugged it out. Have we got to the point where we have agreed on the technology but are now agreeing where it is applied? Or are the developments in how it should be done and the technology that is used still up for grabs?

The Lord Spens: I would say that we are still in the laboratory in terms of blockchain. The door is probably ajar and we are seeing some proofs of concept and real-life examples coming out, but there is a long way to go. The technology is changing literally every week. It is getting better and better every week. People around the world are looking at the technology.

Dr Catherine Mulligan: You can equate it to a database. We have approximately 15 different types of database for sale today. You will probably end up with a similar market for distributed ledgers.

Professor Michael Mainelli: I agree with the database analogy completely. In your previous session, you focused to a degree on the bitcoin blockchain. The performance on that is about seven transactions a second with transactions taking, on average, about 10 minutes. We have blockchains in action at the moment doing about 10,000 or possibly 50,000 transactions a second, instantaneously. So it depends on what you want. We are doing about 60,000 or 70,000 clinical trials with real application, not proofs of concept. We have insurers doing transactions for retail insurance in the Safeshare area, and insurers doing transactions across the reinsurance industry. These are live transactions, going on now. So it is interesting. A lot of the focus has been on payments because many people discovered this technology via bitcoin. The technology is more than 20 years old and there are a whole variety of ways of building it.

Lord Burns: What is the most successful case of this?

The Lord Spens: Bitcoin.

Dr Catherine Mulligan: Bitcoin so far.

Professor Michael Mainelli: I would argue that you must determine what success is. Bitcoin is a very interesting experiment in creating a virtual element. Is it a successful experiment? We will see. I think some of these other applications I am talking about might sound frightfully dull and boring but are doing real work.

Lord Burns: What is number two?

Professor Michael Mainelli: For me it would be the clinical trials area at the moment.

Lord Sharkey: Can I come back to the point that I think you made, professor, right at the beginning, about verification? I am still puzzled by this. I think I understand how verification takes place in the proof-of-work system under bitcoin. I do not understand how in these permissioned systems verification takes place.

Professor Michael Mainelli: Again, there are a whole variety of methods and I might divide them into two. There is a whole group of what are effectively voting mechanisms. We can set up a structure any way we like. We could give the Lord Chairman here the right to authorise every transaction. That is probably close to what digital sterling might look like, if it were built. We can say that we all have to agree, or that there is a cabal of five, or that we need 51%. We can set up any structure we like and the computers will execute that.

The second method is quite different. It is a technique that is still emerging. We call it 'woven broadcasting', but most of these terms are only a year or two old. Blockchain came out only in April 2012, well after bitcoin. This woven broadcasting approach is basically, "How can I fake the existence of a document today that I have hashed?". I actually just record it in the ledger. That is good up to a point for things like time-stamping and document retrieval. So there are a whole variety of mechanisms out there. It is that 'mechanism of validation' where the interesting competition will come from.

Lord Sharkey: And that has a commercial edge to it, too. Presumably the central banks involved in any kind of system, whether it is a digital currency or not, will want a kind of casting vote over verification.

Professor Michael Mainelli: You asked earlier about the role of the regulators. There is an interesting role here. It is certainly something that the Channel Islands have been looking at quite seriously. They issued a consultation document on mutual distributed ledgers last July and they are very interested in this for particular, narrow wholesale markets where there are professionals involved. If Lord Sharkey wishes to trade with Lord Darling in a particular transaction, who am I to say, "Boo"? You are both professionals in the market. What they are controlling is effectively what was spoken about earlier: access to and expulsion from that market. Have you been a good boy or a bad boy? If you are good you can do the trade, if you are bad you cannot. If you wish to trade with me, outside your market, I must go through the procedures to join it. Those are for small professional markets in permissioned areas.

Q10 Lord Forsyth of Drumlean: I think it was Winston Churchill who, when the Comet was brought into service, refused to allow his Cabinet to travel on it on the grounds that he did not want all his baskets in one egg. You talked about the importance of being able to decide whether information is available, the encryption and so on. One of the things we have learned over the years about all these absolutely rock-solid encrypted systems is that 12 year-olds in their bedrooms seem able to break into them. They are vulnerable. Are we not in danger here of creating a huge risk by concentrating vast amounts of information which, if penetrated, will do substantial damage?

Dr Catherine Mulligan: Yes. From my perspective, that is why we always recommend at our centre that we never put data on to the blockchain—yet. The other problem that may occur, which is a long way off, is that once you get to quantum computing all that data becomes easily accessible.

Lord Forsyth of Drumlean: Can you explain that?

Dr Catherine Mulligan: The cryptographic methods currently used today within blockchain for encrypting data would be easily breakable once quantum computing is reached. It is about the keys. You are given a private key and a public key. If I have quantum computing capacity, I can read your private key and read all your transactions. Today, that is very difficult because I do not have the computational capacity. It does not exist.

Lord Forsyth of Drumlean: So to ask the obvious question, you develop these systems and somebody is going to come along with a skeleton key that opens everything?

Dr Catherine Mulligan: Potentially, but if you only ever stored the transaction, all they can see is the transaction and not the data.

Lord Forsyth of Drumlean: But Professor Mainelli said earlier that you have systems where you have both the data and the transactions.

Dr Catherine Mulligan: I will let him speak for his systems but on our systems we have done only transactions.

Lord Forsyth of Drumlean: So you do not think his systems are safe?

Dr Catherine Mulligan: I did not say that. He may very well have quantum protection. I do not know.

Lord Sharkey: Let us just get this quantum thing right. This is not to do with blockchain. Every system we have at the moment that protects any confidential data, including all our bank transactions, is transparent to quantum computing.

Professor Michael Mainelli: That is a very good point. By the way, I think it was Mark Twain, in *Pudd'nhead Wilson*, who said, "Put all your eggs in the one basket and—WATCH THAT BASKET!" This is the point. I helped set up the European Institute for Quantum Computation in the 1990s. If quantum computation hits some of these levels, everything is at risk: credit cards, HTTPS and everything we do will be potentially transparent. We have to watch that, but the structures of this are different.

The Lord Spens: I would say the implementation of your blockchain solution is important. It carries some risks. That is where you should pay attention. There is an element of a third party assuring a board that the solution is fit for purpose and cyber-resilient. But it is more secure than what we have today.

The Chairman: In the two minutes before we must start our next session, Lord Tugendhat.

Q11 Lord Tugendhat: Lastly, what are the opportunities and risks of using the technology to create a central bank digital currency? We have been talking about the risks. Let me just leave that general question with you. How would you answer it?

The Lord Spens: The opportunities would be that you remit money overseas instantaneously.

Professor Michael Mainelli: I would add two things. For the first time, we would actually know the velocity and quantity of money. We have never known that. So that would be a really interesting area.

The Lord Spens: That is a good point.

Professor Michael Mainelli: We would finally see whether macroeconomics is anything other than augury and astrology. It would be quite intriguing at that level. The second thing is novel taxation. You could have a higher tax as you got closer to here. You could have local taxes, or land-value taxes. Of course there is a danger: you could be constantly changing taxation systems as people found that the technology made it frightfully easy to do whatever they wanted.

Dr Catherine Mulligan: Personally, I think there is a lot of opportunity in intra-central banks, so between two central banks. There is a lot of opportunity for those kinds of systems at the moment. I think that is where the low-hanging fruit is. In terms of a central bank crypto-backed fiat currency, I think that that is a lot longer off because it potentially impacts on monetary policy in the sense that it could move money away from the commercial banks towards the central bank. You have to think about that rather carefully, to make sure the commercial banks do not just collapse.

The Chairman: And thereby undermine the current banking system.

Dr Catherine Mulligan: Exactly. So it is a matter of balance, and thinking about what we want to have as an economy.

The Chairman: On that interesting thought, thank you very much indeed for joining us today.

Examination of Witnesses

Mr Simon Taylor, Co-Founder and Director of Blockchain, 11:FS, and **Ms Blythe Masters**, Chief Executive Officer, Digital Asset Holdings, LLC (by video link)

Q12 The Chairman: Ms Blythe Masters, you have described blockchain technology as being analogous to email for money. Can you explain what you mean by that and do you see the technology—I notice that your shareholder base includes many existing players—as a threat or an opportunity for incumbent firms? Would you like to kick off on that?

Ms Blythe Masters: Absolutely. Thank you for giving me this opportunity and accommodating the fact that I am overseas. The analogy that I used here was as much chosen as a way of conveying the magnitude of the business concept as it was a technical analogy. The easiest way to convey my meaning here is to think back to the early days of the 1990s, when the internet was emerging. There was a lot of debate about what the implications of that would be for many different sectors of the economy and companies and businesses. What ultimately happened, of course, is that the internet pervaded everything, with its ability instantly to transmit information all over the world, with implications that went well beyond what anybody could imagine at that early stage.

The reason for using that analogy is that I think the implications of the development of what is more broadly called distributed ledger technology, in terms of potential future application and how it will change many ways of conveying and sharing value as opposed to information, are on the just same sort of scale as the implications of the internet in the early 1990s. We are probably at an analogous stage, meaning that we are in an early stage. The technology is evolving; it is not necessarily obvious or transparent to anyone exactly what the implications will be, but the sense is that, given the power of the technology, the implications will be far-reaching. The comparison with email, which is a way of conveying information, is obviously a very pertinent—albeit not the only application of the internet—

versus what blockchain does. Email conveys information, but blockchain technology conveys value or money or other the assets of values.

There are important technical difficulties that need to be solved when you are talking about sharing or transmitting value and they are more important than when we are talking about sharing or transmitting information. Specifically, when you share information, it is duplicated, but if you share something of value and it is duplicated, that obviously will become problematic. So the technical problem that distributed ledger technology has solved at its very core is how to avoid the so-called double-spend problem. It is not solved at all in the case of email, so in that sense technically it is not a great analogy. So for the technologists or engineers in the room, if there are any, you will have to forgive my analogy—I think you get the bigger point, without my necessarily getting a technical point across.

The Chairman: On the question of a threat or an opportunity for incumbent firms, how would you characterise it at the moment?

Ms Blythe Masters: Again, if you look back to what happened with the internet revolution, the reality is that some businesses were invented because of the internet—for example, Google, Facebook and Amazon. Others were wiped out of existence; for example, Blockbuster, which fell to the online distribution of Netflix and streaming. However, the vast majority of businesses adapted to and adopted the technology and use it in many aspects of their business today. So, for example, if you look at the financial services industry, the notion that one would use the internet for online banking was considered highly debatable in the 1990s, but it is ubiquitous today. My view personally, and certainly the view of the company that I am responsible for, is that there is at least as much of an opportunity for existing or incumbent players to take advantage of the power of the technology to do a better job of providing the services that they provide today at lower cost, at higher speed and with fewer errors and less risk. There will be some that fail to adopt or adapt quickly and therefore, their business model can be put under threat by others who do that. But for those incumbents which adopt and adapt, and because they have the benefit of existing revenues and customer relationships, which newcomers might not have, the chances are that they will prevail and become stronger and/or better. So on balance I tend to subscribe to the school that believes that the opportunity beats the threat. There is no question there are both.

The Chairman: Mr Taylor, would you like to comment on those points?

Mr Simon Taylor: I think Blythe summed it up excellently. The only brief point that I would make is around digital uniqueness. So if I send you an email, we both have copies, as Blythe mentioned, whereas if I take a pound out of my pocket and give it to you and the whole room witnesses that I gave you that pound, everybody knows that there was only one of those pounds—we cannot copy them—and it now belongs to you. That is incredibly powerful when you think about the value of an auditor and the paper trail that exists within banking for middle and back-office processes. That is why people get somewhat excited about knowing who has which value, where and when. From that perspective, incumbents are very excited about it. The organisation that I left is Barclays—I was there as recently as four weeks ago—and certainly that was an area we looked at. From a purely commentary standpoint, Blythe makes the good point that in 1993 you would not have predicted Netflix, and when you look at the new asset classes and the new types of financial services that could be built with this technology, this is an area for opportunity that I have not heard discussed yet today— and is one where encouragement of that and focus on that could be really powerful.

Q13 Lord Tugendhat: It is very difficult to talk about figures when you are talking about something that is at this stage of development. We have been given figures that suggest that the annual cost savings for clearing and settlement could be of the order of $16 billion. It seems to me that figure could very well have been plucked from the air, but how does it sound to you?

Mr Simon Taylor: I read the report behind that. I think that the science was quite simplistic, in that it looked at the cost of post-trade and said, "If we took these bits out of post-trade, what does that amount to?" So it was a simple calculation but at the same time the technology has the potential to do that. Again, I would say that that is overly simplistic. If you look at the entire trade life cycle, what you could do could be far higher than that. If you look outside capital markets, the number could also be far higher. If you look outside exchange trading and over the counter, you start going to commercial banking, retail banking and so on. So I think that that number is realistic but it assumes that we would displace all the post-trade, which I think is probably unrealistic. We may make back-office and middle-office processes inside banks a lot more efficient, but I would question over what time horizon. Are we closer to five or 10 years than we are to three years? I am aware of some initiatives in certain geographies that may be able to concentrate that and happen

faster, but across the entire industry it would take a long time to knock that cost down. There may be a shorter-term benefit. If you are a large organisation encumbered by costs, whose business model is suffering as a result of a depressed interest rate environment and you have progressively more reporting requirements coming towards you, a technology that is effectively an auditor and does reporting could be tremendously interesting as a kind of wedge product in 12 to 18 months' time.

Ms Blythe Masters: If I may interject, I agree with Simon's point. The origin of that figure that you quote is a research report put out by Autonomous Research, which is an independent equity research firm. Its estimate is derived from the total back-office cost of the major global investment banks—by no means all banks, just the big global ones. It assumes that 30% of costs associated with clearing and settlement, custody financing, books and records, reference data, reconciliation, corporate action, tax and regulatory reporting could be cut. All those areas of expense are definitely addressable using this technology. A 30% estimate of that total over time, as Simon said, is not directionally incorrect and is the right order of magnitude. I also agree that it is only looking at a subset of one industry and the subset costs in that one industry. It then only estimated that 30% of those costs would be reduced in a decade—by 2021 or so, which is not tomorrow. I would suggest that that estimate is based on purely speculative analysis, but it is a reasonable foundation.

Lord Tugendhat: Can I ask a follow-up question? You drew our attention to the internet as it was in the 1990s, so I follow that analogy. One thing that strikes us about the age of the internet is the growth of enormous monopolistic organisations—the Googles, Microsofts, Facebooks and so forth. Inevitably, therefore, in the light of your analogy, one wonders whether the private sector might not coalesce around one distributed ledger for clearing and settlement, and that one would have again a monopoly at the heart of an activity.

Mr Simon Taylor: That is entirely possible, although not likely from what I have seen in the market and given my opinion. I think that there are different markets taking different approaches. Somebody mentioned VHS and Betamax. I think that is already happening. We are in an experimental phase. The ability to get everybody to adopt the same thing is just hard. To get significant momentum, you often need to find a problem that is not too big and not too small. I suspect that that is where Blythe's organisation and some of Blythe's competitors are looking for those problem statements. If there are then many blockchains, the question is whether they start to interoperate. Is there some kind of standard? This is

what R3 are working on with Corda and it is what the Hyperledger Foundation is working on. There are many other efforts to do the same. If we have these many ledgers and there is a protocol that binds them all together, could you start building natural monopolies over that? That is a fair question, but it is a second or third-order question maybe 15 or 20 years down the line. I do not know honestly how you prevent that other than to say that, from a regulatory perspective, you do not want to create one world bank and you do not want to centralise one balance sheet. If anything, this is moving away from that systemic risk that we have seen in the market. We have seen a move towards CSDs and CCPs and one balance sheet. We are now seeing a move towards the repatriation of that liquidity with the banks and a separation of some of these commodities in the marketplace. That is my view.

The Chairman: Blythe, would you like to comment?

Ms Blythe Masters: Yes, I would be happy to. On balance, if you look at the impact of the internet on most businesses, it has been a promoter and a driver of competition through essentially levelling certain playing fields. For example, the FinTech revolution is fuelled in large part by advances in the internet, big data and so on. As to what it is doing to the financial services industry, I think that you need to speak to the chief executives of any major financial concern, and they will say that the internet is a major source of competition and competitive stress. So in that sense I think that the internet has brought at least as much competition as it has monopolistic concerns. I cannot yet think of, in my mind, an analogy to a company such as Google with its dominance in research in the context of distributed ledger technology, although obviously one's power to imagine the future is limited, as it was in the early 1990s, when I do not think that anybody imagined Google in the early 1990s, so I would not rule it out, as Simon said.

There are a couple of things. First, there is no reason why, logically, we should evolve to a situation where there is one ledger to rule them all. There is no real business reason for that, unless it were the case that as Simon points out that separate ledgers meant that the information or store or value on those would not ultimately be interoperable which means that information in one ledger could be transferred safely and securely to another ledger essentially embedding that value in a different form. If you achieve interoperability, which is a big bonus of the industry right now, there is no reason to expect that you would end up with one ledger provider and one ledger to manage all transactions. I think that that is highly

unrealistic. I think what is much more likely is thousands, if not hundreds of thousands, or millions, of distinct ledgers that are able to interoperate.

The last point is that this area is very much characterised by the fact that the technology itself was inspired by open-source community projects, such as the original Bitcoin blockchain. Many aspects of the technology development are going on in the open-source community today—the Hyperledger Project is one example. The technology developed there is intended as the fabric on which competing entities can build their applications and it is being developed as open source for free, essentially, for use by anybody. I find that very encouraging. I think that it reduces barriers to adoption. It is one reason why our company has been very supportive of that initiative and has contributed code to it I think that that will to a large extent mitigate some of the concerns that you are raising.

Mr Simon Taylor: The internet itself is largely fragmented. It is a network of networks by its nature. Similarly, I think we are both saying that that is the way the distributed ledgers will start to look: a network of ledgers, as such. That is not to say that somebody could not build a monopoly in a new asset class or something we have not predicted yet, but it is certainly not what we are seeing in the market currently. But on Blythe's point, if you wound the clock back to 1993, we would probably have said the same things about the internet.

Q14 Lord Forsyth of Drumlean: How can the transition be made from the current settlement system to a blockchain-based system? What risks will be involved in making that change?

Mr Simon Taylor: The transition really depends on what problems you want to solve first. Because there are different types of money, you could start with central bank money, do a central bank's books and records, and issue value directly into the balance sheet of a bank. However, that may be a particularly difficult way to start. There are probably simpler instruments from which banks are trading these on each other's balance sheets on a day-to-day basis on a given exchange. So I suspect it would be something where you have a relatively simple and uniform instrument. Perhaps this might be a commodity, like gold bullion. Perhaps this might be a standard instrument like the interest rate swap or credit default swap, something that is largely quite standard and could be traded.

You could start to automate the legal document process rather than the settlement initially. You would baby-step your way towards the settlement at the end. So you would say that you and I have to agree this contract. Today, we do that with lawyers and paper and emails.

Let us move that bit on to this new system and then let us come to a shared agreement about that. Perhaps we settle that through SWIFT, as we do today, for a period of time. But actually what we find over time is that, because we have this digital record, we can start to authorise settlement with prefunding of that transaction or settlement from somewhere else in this closed network. You start to do interesting things there. That is what you are seeing inside some of the consortia and with some of the companies like Blythe's. They are working their way towards settlement, de-risking the approach as much as they can in baby-steps. So I would say it is those types of transactions—interest rate swaps and CSDs—but also the commodity space, maybe commercial paper, and starting with the legal document automation.

Ms Blythe Masters: I'll perhaps illustrate that is by giving a real-world example which is under consideration currently. I want to emphasise that I am speaking now in generic terms about dealing with proposals and business designs that my company is be responsible for, rather than speaking for any of our clients here or specifically ASX. I mentioned the case of ASX, the Australian stock exchange operator, because it is in the public domain that it is considering the use of distributed ledger technology to replace its existing post-trade clearing structures for the Australian cash equities market. I do not want to suggest it is a decision that has been taken at this stage. They might approve it in the next session. It is an example project.

Obviously, the first point to make is that that kind of market infrastructure is a systemically significant consequential market infrastructure for the economy, as are most national stock markets. And in Australia, just like in the UK and most other jurisdictions, those market structures are already subject to a substantial body of regulations, much of which is focused on the containment of systemic risk. If you want to put yourself forward in decisions regarding the systemically consequential market infrastructure, you have to keep a lot of regulators—in the UK there is only one regulator—happy in terms of your ability to answer important questions around security, privacy, redundancy, reversibility, recovery, contingency, performance and so on. That is good news, because anybody who is seeking to replace an existing market infrastructure with the new technology has a roadmap to follow in cracking the necessary solutions that are well known and understood. In the event, if your answers or solutions fall short in any of these dimensions, the simple answer to, "Can I use this alternative technology?" will be "No". So I think that is an important point to make.

Essentially, there is an existing body of regulations to ensure that the systemic market infrastructures do not wake up one morning with a new, untested, unproven, unfashioned framework.

Lord Forsyth of Drumlean: Just to put this quite crudely, but with specific operations or specific types of commodity transactions I can see how it would be possible to make those systems more efficient using this technology. It sounds to me as if the idea that we could move everything from the current settlement system into a blockchain-based settlement system and make huge savings is a bit of a fantasy because the risks are too great.

Mr Simon Taylor: Potentially, but you may look at it as part of an upgrade cycle. So, if you have to upgrade a systemically important piece of market structure, as Blythe says, then maybe you consider this technology as part of that upgrade. You might have ASX, but there are many other market infrastructure providers looking at the same technology, such as DTCC, CLS, Euroclear, Clearstream, to name a few. There is an opportunity to run the blockchain technology alongside your existing settlement infrastructure and gain some benefits in reporting and transparency. Then over time, as central banks, regulators and the incumbent banks become more comfortable with that technology, you could start to move settlement in that direction, as you have more certainty over the legal status of a smart contract, for example, or of settlement finality. There is some good work on that.

Ms Blythe Masters: I would add to that, so that it is consistent with my earlier response. Each of the dimensions of market infrastructure can be addressed securely, credibly and in a responsible fashion by making particular classification choices that use some, if not necessarily every aspect of, distributed ledger technology, you may have read about it in the newspapers. I think one of the earlier speakers spoke about the distinction between the running of the Bitcoin blockchain with its design and features versus private or permissioned alternatives, whereby the notion of encountering anonymous actors or infrastructure operators is removed entirely by simply requiring that all participants are pre-credentialed, have entered the club in advance and are known with certainty, including by the regulators.

There are also mechanisms for ensuring the recoverability and reversibility of the information. So if the system goes down, is there the capacity to ensure that it can be recovered and in a short enough period of time? If an error is made, is there a pre-approved framework to ensure that can be reversed in a fashion that is consistent with the rulebook of the relevant market infrastructure? Also, I think your earlier speakers emphasised, and I

strongly agree with them, the fact that privacy is vitally important in the case of settling large volumes of financial activity. Not storing sensitive contractual information on a shared ledger is definitely a feature of the recommended design that we are working with in order to avoid any possibility that, either through quantum computing in future or other forms of leakage, that sensitive information could be leaked. It is simply not stored on the ledger. What is stored on the ledger in order to effectuate parts of the post-trade settlement process is proof of a hash of transactional information whereby, only the entities impacted are able to interpret that proof. Even if you were able to compromise their understanding of that proof, all that you would know is that a transaction happened. You would not know the key data, the economic terms of that transaction: the price, the volume, the time, the decision and so on.

So this is a very technical space. You need to have a deep knowledge of the way in which capital markets work today and the risks that they present in order to be able to design systems that adequately tackle those risks. I have spent the better part of thirty years dealing with the financial services industry breaking data down and control roles and running businesses with a heavy reliance on technology, and I am very comfortable that design choices selected from the options available within this broad area are absolutely essential from the point of view of materially reducing existing risks. [INAUDIBLE] Again, these are the details [INAUDIBLE] that are necessary to judge these things correctly.

Lord Forsyth of Drumlean: You will forgive me for observing that we were told similar things in 2008 about financial instruments reducing risk, based on models that turned out to be inadequate.

Q15 Lord Sharkey: Could you talk a little about smart contracts and what benefits they might bring? It would help if you could give us some examples of these things in operation.

Mr Simon Taylor: Sure. "Smart contract" is a misleading term, because it implies a legal agreement between two entities. In some cases, it might eventually become that, but I suspect that what we will actually see in capital markets is a few flavours of interorganisational workflow. That is a lot of syllables, but what I think I mean by that is that today there is no way to drive a workflow between bank 1 and bank 2 and make sure that what has happened here is reflected here. Forgive me, Blythe, for doing a hand movement here. There is no way to drive that workflow. If we have interorganisational workflow, we know the state of an agreement at a point in time, and, as I think Lord Patrick Spens said,

you could then start to make a workflow decision. "If the price of this index goes above X, move collateral from A to B" would be the classic example. You might say on the shared ledger, "This bit of computer code now owns this value". It is like a corporate being a legal person, but actually there is no human.

Similarly, a piece of computer code could take custody of an asset and then manage its workflow. I suspect that that is very far off, because there are a lot of legal consequences in doing that. What we will probably see in the short term is that legal contracts actually delegate to computer code. I want to buy a commodity from you, and you and I come to an agreement that if its price goes above X, I will move margin one way, and if the price goes below Y, you will move margin another way. We would come to an agreement in a way that is not too dissimilar to the way we do now. We might change the paper process into something that is more digitised, but we would say to the software, "Watch this data feed from Bloomberg, Thomson Reuters", whomever it might be. If that data feed changes to be above X or below X, you have the ability to change the value in one account to the value in another account. You can settle the transaction. Now you have an automation of the backend of that agreement.

Lord Sharkey: Why do you need blockchain to do that?

Mr Simon Taylor: You do not need a blockchain to do it, but a blockchain makes it a lot more efficient. The problem at the moment is that there are many core systems that do not really talk to each other. Either I have to have one entity that manages all that workflow and agrees it, or I have to have everybody adopting one standard. Centralising all the workflow for all the banks in all the world will naturally be quite hard. Standards are at their best when they are very simple, so it would be too complex to get a standard adopted that could drive a series of complex workflows for every different type of bank. The beautiful thing about a contract is that, per this one set of agreements, I can set some "If this, then that", but I can also say that the system that sits out here—this distributive ledger that controls my money—we are just going to reference it. We are going to sign the distributive ledger, then we are going to reference it, then it has permission to follow the instructions that we have given it by the fact that we have signed it. Today, I would say to a central authority, "I am going to sign this and you can do it", but that authority would not be able to change my systems or the other banks' systems. Here, I have said to a CCP or an exchange that I want to do this. I might also have said it to Thomson Reuters or somebody else. I have also been

given permission by both the banks to update their systems and drive the workflow inside their organisations. That is the bit that is new, in my mind.

Ms Blythe Masters: I would like to go back to the prior observation, which I respect deeply, that in 2008 and before then there was a lot of commentary about new bank rules for financial instruments potentially reducing risk and about the chain of transition elements, if you will. I think that very important lessons were learned as a result of that experience, and if I were to summarise those I would say that there are a few things that have informed some of the objectives of the work that we are trying to do in this space today. Number 1 is a lack of transparency in the nature of the contractual relations between entities, which made the job of the regulators in understanding the risks in the systems almost impossible. Number 2 relates to the interconnectivity between institutions and the potential for the contagion of risk, which led to fear that paralysed the markets. Number 3 relates to the nature of the transactional instruments that you referred to that were used to transfer market-critical treasury between institutions in a way that, again, lacked transparency.

The difference here is, number 1, that the systems are designed in a way that the intention is to give a regulator or regulators the ability, on an unprecedented scale relative to what they have today, to access information in relation to the interaction between parties. Not just from the point of view of transactions that are simply buying and selling but from the point of view of unsettled obligations that create risks in a stressed market environment. We are talking here predominantly about post-trade processing—all the other back office stuff that happens between the point at which you say done on a transaction or you get fulfilled on the transaction, and the point of time two or three days later, or sometimes more, when the legal completion of that transaction is effectuated. Having a regulator with a real-time view into that and being able to interrogate it rather than gathering post-trade reporting and trying to aggregate it is a significant step forward in tackling aspects of the transparency problem that have not yet been resolved, despite the good intentions of the post-crisis reforms. I want to emphasise that that was the genesis of my earlier comments about risk reduction, and I agree profoundly that the lessons of 2008 are affecting the treatment of financial institutions and regulators looking at this space today.

Finally, turning to the question on smart contracts, one of the challenges of smart contracts is the notion of allowing the contracts to self-execute in the distributed network without intervention and the importance of ensuring that if you do chose to put contractual

information onto a distributed ledger, how can you be absolutely confident that the transaction will be kept private. This is the kind of information that is sensitive and market-moving. This is why, in my earlier comment, I referred to not putting smart contract execution capability on to a ledger or on-chain. Rather, at this stage, until we can be confident of that privacy protection keeping that information off the shared ledger, and mostly conveying to the shared ledger a notification and synchronisation tool, which is essentially a hashed proof of the fact that a transaction having occurred that satisfies the contract. That means that that information never makes it way directly onto the ledger and therefore cannot be interpreted by someone who compromises it. That is an example of one of the security parameters that I referred to earlier [INAUDIBLE] so that the regulators can get comfortable with the transactions. The idea here is simply avoiding the probability that contractual information can leak by not putting it on the shared ledger.

The Chairman: Thank you. Two follow-up points: Lord Forsyth and then Lord Darling.

Lord Forsyth of Drumlean: Thank you for addressing my slightly pointed comments about 2008 and risk. I get what you say about the regulator being able to see in real time what is going on. Surely the volume of material will be so immense that you will need, say, a large number of insomniac regulators. How are they going to process this information?

Ms Blythe Masters: Good question. So today, and I believe you have representatives of regulators in the room who could probably attest to this, there is a body of regulation around the world in this area, so economic [INAUDIBLE], which requires a mandate for post-trade reporting on all sorts of activity. That is all happening currently, bilaterally or individually. As a result of the regulator being more particular, there are incoming delays with reports that are in a variety of formats which quite often do not speak to each other and are quite often are subject to errors due to the transmission of data being an inherently error-prone exercise. The regulator on the receiving end of that has to aggregate that information and then somehow interrogate it. The fact is, it is current information not just data. That is the case today.

You may have even read in the United States, in the FEC where the burden on appeal was blocked the day before in the [INAUDIBLE] market. Basically, the failure came about because it does not have the typical computing power to cope with the analysis needed to interrogate the post-trade recording accurately. What is being suggested here is that instead of that bifurcated reporting after the fact, with multiple different entities, you provide a

regulator with not only access but a user interface that is linked to that reporting tool and that can interrogate data. To give you a very simple example, imagine that a regulator investigating financial crimes would like to be able to see the total activity of one ultimate beneficial owner across securities activities. Today, that is really only possible in most jurisdictions by a process of interrogating, by subpoena or otherwise, the records of individual financial brokers and intermediaries. You then have to spend weeks getting together statements which may or may not give you the full picture. That picture could be provided on a real-time basis in a world with distributed ledgers, where a regulator was provided with a permission to view. But you are absolutely correct that the quantity of information we are talking about is gigantic. It is already gigantic. It will not go up as a result of what is being recommended here. It will become more analysable and more readily interpretable as a result of what is being recommended here.

Q16 Lord Darling of Roulanish: Blythe Masters, you gave a very lucid explanation at the start of your evidence of the evolution of the internet and blockchain. I am quite sure that blockchain could bring many advantages, but would we not be kidding ourselves if we believed, just because all the information is out there somewhere, that somebody will actually take the trouble of reading and interpreting it? Without going over old ground, in 2008 the information was there for all to see. However, people chose to ignore it because it did not suit them, whether they were regulators, banks or governments. It was not that it was not there; it was all too clear, but was just ignored. My question is twofold. First, what ought the Government to be doing to facilitate this? Also, what should we be wary of? I think we would kidding ourselves if we thought this was the answer to all our prayers. I do not think it is.

Ms Blythe Masters: That is an excellent question. I think that there is a need to stipulate to the systemically consequential market infrastructures, the ones big enough to impact the economy of the world, the ones that are taking up macroeconomic variables and so on that there should be intense scrutiny at this stage. As I mentioned earlier, the good news is that the authority to do that is already in existence. There will need to be a period of extensive education and proofing out of technology before anything that has any semblance of actual implementation is committed. My belief is that many features of the original invention, which is why all this works—namely the public Bitcoin blockchain—are profoundly

unsuitable for use in these contexts. But those are just the technology specifications and they can be changed.

At the end of the day, the way I like to think about this technology is that actually it is a very basic concept. It is nothing more or less than a new form of database technology. You all know what databases are and how we use them. They have certain features that, traditionally, we as users find problematic. They are centralised, they are administered by one entity. That entity usually has unilateral editing powers. They can go back and correct something for benign reasons or for malicious reasons. We have no ability to prevent that happening. The data inside is typically unencrypted so perimeter security becomes important. Often enough, you read that the perimeter security is vulnerable to penetration. We all know what happens after that. The lucky ones are the ones that know they have been penetrated, and the unlucky ones are those that do not yet know. But the feature of database technology is such that it is vulnerable.

The other feature of it is simply that it is not, in the case of current database architecture, realistic or responsible for distinct, particular institutions in different parts of the financial ecosystem to rely on a shared or mutualised infrastructure, because they are unable essentially to independently validate a fact as it relates to their activity if they are relying on someone else to keep a record of that accuracy. The result of that is that we all keep our own separate databases with the same information, and then waste literally billions of pounds a year, and dollars, around the world on reconciling that information. If you could introduce a mechanism whereby it becomes possible to synchronise and notify different parties in such a way that they are able to independently, without anybody else's help, consider and confirm whether the activity declared to be theirs was actually authenticated by them, then you introduce the ability to mutualise the infrastructure. That eliminates processing rates. All of the time that it takes in reconciliation with respect to checking two different records of the same activity goes away— because now they are the same. Reconciliation can be avoided. Now, what you are checking is whether you agree with the one record of the activity that affects you. That leads to radical reductions in error rates. It is error rates and the need to resolve them that lead to the delays and latency in settling financial instruments. That, in turn, is one of the lead capabilities within the financial markets which has not gone away in the post-crisis reform era.

We have materially improved the situation with respect to derivatives by transactional reporting and central clearing and margin requirements, but settlement itself has not been tackled yet at all and remains a relatively archaic process by comparison. So that, in essence, is what they propose here: a more secure, shareable mutualised database infrastructure that granularly ensures privacy through encryption techniques, but where the data itself is kept off-chain and proof of that integrity and synchronisation of it are on-chain. That is a unique, extremely clever and very different way of thinking about managing information. It is strictly superior to the multiple-sharded databases that we use today.

Mr Simon Taylor: I consider blockchain a great auditor or reg tech. How do I know what is in your database? I do not. Actually, one of the things from an auditor perspective is that I need to know the exposure between banks and certain high-level bits of information, but I do not need the absolute detail of everything going on underneath it. That is the point that Blythe was making.

In terms of the second part of what the Government should be doing, a lot kicked off on the back of the Government Office for Science Blackett review into blockchain technology. There was a lot of stuff in government departments. One thing that I would suggest is that there is still probably a need to understand the smart contract side more. I know that there is some work in the department formerly known as BIS to really kick that off. A shared legal understanding of that would be very helpful, and forums for that knowledge transfer would be tremendously helpful. In the environment we are in now, there is a real need to foster the start-up ecosystem. London has a very vibrant blockchain community. I have had the good fortune to meet many people from it. If we can give visibility to and promote that, that would be tremendously helpful. What will the challenges be? That is a fair question and needs to be considered. Any change in an incumbent organisation is very difficult when you have millions of customers and legacy IT.

On the point about how you start to adopt this technology, the reality is that you have to start running it alongside your existing processes. That is why the analogy of having this almost auditor that runs alongside and keeps track of it is a really key wedge and integration point. Then, the actual integration between the bank systems into a shared ledger will also be a non-trivial challenge to resolve.

The Chairman: We have time for one last question.

Q17 Lord Turnbull: This question continues the question of what government should be doing. Are there any specific prohibitions in the system that it needs to be remove, just as at one stage we had always had to sign a cheque and gradually we got rid of that? Are there any things that you would definitely not want the Government to do?

Mr Simon Taylor: I will answer from my own perspective. They have been doing the right things so far. Indeed, the Governor of the Bank of England's Mansion House speech on creating an accelerator for start-ups was very helpful. More publicity around that would be useful, but it is also about the competitions and grants for the start-ups that are out there, and working with universities to bring this through. That has been happening, but it has been happening very slowly—there is a need to accelerate that. There are pockets of knowledge inside industry, academia and the start-up space, but government as the communicator across those could be tremendously helpful.

As for the signatures piece, work has started around legal precedence or the potential to use a smart contract as a legal agreement. Giving that some visibility and air via the work that is going in what was formerly known as BIS could be tremendously important for financial services. We should progress legally enforceable contractual agreements.

In terms of things not to do, again, it would be the usual: do not rush to regulate or standardise. The technology is still very early and we are at least a couple of years away from being able to set a standard. We need to allow industry and the start-ups to continue to experiment for 18 months to two years. We will see the beginnings of the first commercial implementation. Anything that can be done to encourage that is a good thing, and then reacting appropriately as it evolves.

Ms Blythe Masters: I have a hard stop at 12.30 US time—in about five minutes; my apologies.

In terms of our current impediments, I do not see any major restrictions. I do not see any current explicit impediment or need for changed regulation that currently stands in the way of the development of the technology. In terms of innovation and development, I would echo Simon's comments. I think what the UK is trying to do is extremely constructive and will serve the UK well in the long run as a magnet for innovation and financial trade. One thing that rarely gets brought up by these groups is that a lot of the consequences of the technology change that is happening here will have implications for jobs, particularly the lower paid, less value-added jobs within financial services, for example. That 30% that will be

saved is principally going to come from back office jobs that will be automated. This raises the same question that we have been dealing with since the agricultural revolution and then the industrial revolution, about what the introduction of technology does to employment. At a government policy level, there will need to be a continued focus on investment in education, in science and technology, engineering and maths in particular. As we know, looking at other countries round this world these are not as strong as they could be. We should look at whether there are significant gender biases in the representation of women versus men. This would be an area of focus that would have longer-term implications for job creation and productivity that go well beyond the capacity of technologists to think through.

Q18 Lord Lamont of Lerwick: I want to ask about a central bank digital currency based on blockchain technology. Again, we are talking about interbank payment systems. I gather that the view has generally been expressed that the savings from such a move would not be as large as those from exchanging securities. What if this central bank digital currency was widened so as to compete for commercial bank deposits? I gather that Mr Broadbent—unfortunately I could not be here when he spoke earlier—has argued that that would have profound implications for the structure of banking and perhaps call into question even fractional reserve banking on the grounds that the assets would be as liquid as the liabilities. Do you agree that it would have this profound impact and implication for the commercial banking system?

Ms Blythe Masters: I believe that the two matters can be separated into a distinct technology response and a policy response. If you wanted to introduce a central bank currency, that would introduce efficiencies and some of the other things that we have been talking about. Although, as Dr Broadbent earlier pointed out, the order of magnitude of savings that come from the cash currency side as opposed to the securities side is far smaller. So it would be a simplification and a positive, but it is not necessary to achieve the cost savings that we have been talking about. It is not a necessary feature of any of the businesses that we are testing.

As a policy matter, if you were to introduce digitised pounds, for example, the question simply becomes: to whom do you give access to central bank money? Do you gradually narrow the field of banks that enjoy that privilege, or do you expand that dramatically? That is not a technology decision; that is simply a policy decision. If you were to expand it dramatically, there absolutely are implications for the entire structure of the banking

industry [INAUDIBLE] If there are millions of them doing it, that then leads to enormous implications for the role of [INAUDIBLE] These are very interesting points, but I do not think they are technology decisions; they are policy decisions.

Mr Simon Taylor: It really depends on how you design it. You do not have to design it so that it displaces fractional reserves—that is a design and policy question, as Blythe rightly points out. Some of the advantages of moving towards a central bank issue of digital currency might be that you move towards a cashless economy with the associated reductions in fraud, and potential receipts in taxation, but then you might have an adoption question—people would start stuffing cash in their mattresses and so on. I understand that one of the goals of the GovCoin pilot is to observe and figure out whether you could do things with financial literacy and create a user experience that was so enjoyable that people would prefer to use it rather than cash. It is a fair question and I would not confess to know the answer.

If you are to take on the central bank being the liquidity provider for the market and competing with commercial banks, that creates a systemic risk that is bigger than the existing "too big to fail" model that we have today. Now, you are effectively putting that entirely on the sovereign. That distribution within fractional reserve can be useful, but also the fact that you are fractionally reserving can be not useful. That said, the goal of people looking at this in the Bank and some of the research departments is to have visibility of how fractional reserve is being apportioned throughout the financial system. What one bank's liability is to another may be where they wish to start. If they want to open up central bank money to payment service providers and other intermediaries in the industry, could they then have traceability around those interbank liabilities and asset flows?

Ms Blythe Masters: My apologies, but I have to leave the conference. Thank you for giving me the opportunity to contribute. If there are additional questions, I would be happy to address them in writing.

The Chairman: You are very kind. Thank you very much for joining us, and, Simon Taylor, thank you very much for joining us in person.