Science and Technology Committee

Oral evidence: Blockchain, HC 467

Wednesday 29 June 2022

Ordered by the House of Commons to be published on 29 June 2022.

Watch the meeting

Members present: Greg Clark; Aaron Bell; Chris Clarkson; Tracey Crouch; Rebecca Long Bailey; Carol Monaghan.

Questions 1 - 94

Witnesses

I: David Shrier, Professor of Practice, Imperial College Business School; and Izabella Kaminska, Editor, The Blind Spot.

II: Dr Tom Robinson, Chief Scientist and Co-founder, Elliptic; and David Gerard, Journalist and Author.

III: Professor John Naughton, Senior Research Fellow, Cambridge University Centre for Research in the Arts, Social Sciences and Humanities; and Craig O'Kane, Chief Operating Officer, Everledger.

https://parliamentlive.tv/event/index/5f598dbb-6fa9-4d49-bf5a-70f9efca3192

Examination of witnesses

Witnesses: David Shrier and Izabella Kaminska.

Q1 **Chair:** This morning, we have a session concerning the origins and key questions for policymakers that arise from blockchain. To help us to answer those questions, I am very pleased to welcome our first pair of witnesses: David Shrier, Professor of Practice in AI, artificial intelligence, and Innovation at Imperial College Business School here in London; and Izabella Kaminska, the editor of a website, Blind Spot, which focuses on finance markets and media news, with a focus on technology. Izabella is an alumna of the *Financial Times* and spent 13 years, including most recently as editor of FT Alphaville, the *Financial Times* markets and finance blog. Welcome, both of you. Thank you very much, indeed, for helping us today.

David Shrier, briefly describe how distributed ledger technology works.

David Shrier: Thank you, and good morning. Distributed ledger technologies or blockchain were born out of the 2008 financial crisis. A group of technologists had lost trust in Government and in banking systems, but they trusted technology. They wanted to address issues of trust, transparency, security and privacy. They created a kind of database; you can think of it as a set of ledger books, with many copies.

The copies are all talking to each other. Because they are constantly double-checking the information with each other, this is a much more secure way to manage information. The copies can be public, which promotes transparency. People can verify what is in the ledger book. If we are moving money around, we know where it is coming from and where it is going to.

The original application of blockchain was something called Bitcoin, which is a digital currency. Since the advent of Bitcoin almost 15 years ago, however, a number of other use cases have emerged, including better collection of tax, improving supply chains, securing digital identity and even accelerating biomedical research.

Q2 **Chair:** Thank you. You say it came out of a lack of trust in Governments and financial institutions. Perhaps you will say a bit about how that trust problem is remedied. Is it also the case that, as well as the consequences of a lack of trust, potential savings can be made if you do not need to route transactions or ledger entries through a trusted third party? Is that right?

David Shrier: Absolutely, Chair. Your question hits at the heart of how this emerged, because if you think about the conventional financial system, there are a series of intermediaries. If I want to send you money or you want to send me money, it has to go to a bank, to a central bank, to another bank and to you—many intermediaries with a lot of obscure practices for the average consumer or individual. With the cryptocurrency application of blockchain, I can send the money directly to you and we

can both see that it left my wallet and it arrived in yours. Technology secures that transaction.

Q3   **Chair:** How is that trust replicated? How is it confirmed?

David Shrier: I will call it algorithmic math. There is a series of calculations that are performed to make sure we all know the money left my wallet and arrived in yours. In conventional financial services, we trust HSBC or Barclays to tell us that it left my bank account and eventually arrived in yours. Here, we are replacing all those intermediaries with technology, which means we remove many layers of cost and delays in time in order to move money. For example, there is over $10 trillion of money floating around between countries as we try to move money across borders. It takes as much as three days. With the blockchain technology, you can move that money in a matter of minutes.

Q4   **Chair:** Without getting impossibly technically detailed in doing that, how do you verify that the transaction is proper and can proceed? It involves the use of a public key and private key to validate an entry. Can you explain how that works?

David Shrier: Absolutely. There is some cryptography that protects my money and protects your money. There is also cryptography that protects the record of the fact that the money left my wallet and went to yours. That is incredibly important because we do not want to spend the money twice. If we do not have a good record of the fact that I do not have it and you do, then I could spend it, you could spend it and the whole system would collapse.

There is an algorithm, and the most popular algorithms are either proof of work or proof of stake. Either way, you are using a calculation that gathers up a bundle of transactions. This is why it is called blockchain: you are creating a block of transactions. It calculates the fact that I am giving money to you, he is giving money to her and so on.

The blocks are then stitched together in a chain. If you try fiddling with one of the blocks, you will break the chain, effectively. I am over-simplifying, but you are using this set of calculations to make sure that we have an accurate record of where the data is moving—in this case, money.

Q5   **Chair:** I see. What is it about it that prevents that record from being fraudulently manipulated? What makes it impossible to change?

David Shrier: To vastly over-simplify for the sake of this discussion, when it is performing the calculation that keeps track of the money moving around, it comes up with a number. Recall what I said earlier about there being many copies of these ledger books recording transactions. That number that says that the money went from me to you is copied into all those ledger books. If you wanted to subvert that transaction, you would have to change the information in thousands of ledger books all at the same time. That is how we would secure it,

because the validation of the fact that something happened is distributed across many, many different end points, which makes it practically speaking very difficult to hack.

Q6 **Chair:** Surely with a large capacity of computing power, just as it is possible to make a legitimate change to multiple ledgers, how can that not be done fraudulently?

David Shrier: The current encryption is what is known as 256-bit encryption. It would take a galaxy of super computers twice the length of the life of the universe to crack that code in order to break the transaction. However, once quantum computing becomes practical, it could do it in a matter of minutes or seconds, which is why people are thinking about what happens when quantum becomes practical. Today, quantum is not practical, and, today, that 256-bit encryption, which also is what secures Barclays, HSBC and others, is adequate to purpose.

Chair: Thank you very much, indeed.

Q7 **Rebecca Long Bailey:** Mr Shrier, you mentioned that the origins came from the 2008 financial crash. One of the reasons for that crash was the packaging together of derivatives—a lot of bad debts topped off with a few good debts. How would this technology address that issue? Would it go down to the level of detail that shows how banks might be trying to package up the debts in the same way as they were then?

David Shrier: There is absolutely the potential to apply this trust and transparency function to that problem. At present, it is not being used widely in that use case, but there is certainly a potential to do that.

Q8 **Rebecca Long Bailey:** What risks or abuses can you foresee within the system that potential banks might use to circumvent transparency? How can that be addressed?

David Shrier: There are a couple of key risks and a couple of mitigants. First, this is fairly sophisticated technology and it is a new financial security. For the average consumer, if they do not have education about it, there is the risk that if they are buying or selling these cryptocurrencies they could be outmanoeuvred by very sophisticated traders in a bank. In the same way as if they are trading equities on a listed security, they could be out-manoeuvred.

This is a place where regulation and Government oversight can provide some protection for the average consumer. Although I do caution against over-regulation, I am in fact a fan of regulation because it provides clarity to the industry.

Another mitigant is the technology itself. There are a lot of websites, technologies and tracking systems that can let people see when large amounts of Bitcoin or Ethereum or other cryptocurrencies are moving around. That can provide an early warning signal to somebody that

something is afoot in a way that we do not have in conventional equity or debt securities that are publicly traded.

Q9   **Rebecca Long Bailey:** To ensure we all understand the technology, from what you described so far, it seems to suggest some large database, a massive worldwide ledger that simply documents transactions. Is that right, or is it more complicated than that?

David Shrier: That is one application or foundation layer of blockchain technology. There are many other applications, not just the currency and security applications we are talking about. I do want to emphasise that blockchain is not Bitcoin; cryptocurrency is not blockchain. These are subsets. However, they are multiple databases, and sitting on top of them are systems to access that database—trading exchanges, wallets. There are several layers to it, just like there are several layers to the conventional financial system.

Q10   **Rebecca Long Bailey:** What differentiates the different types of blockchain from one another?

David Shrier: We often refer to them as protocols. One of the core points of differentiation is: how do we calculate that complex math I was talking about? Is the protocol proof of work, which is primarily used by Bitcoin, or is it proof of stake, which is used by many, many other varieties of blockchain? Proof of stake is interesting because it is much more energy-efficient. Concerns have been raised around the energy usage of blockchain, and proof of stake is one mechanism to address that.

Q11   **Carol Monaghan:** Izabella Kaminska, you have reported extensively on the use of blockchain. How has interest in blockchain changed over the last few years?

Izabella Kaminska: That is a good question. We were talking about 2008, and in the early days almost no one had heard of it. In fact, the first case of its proper application was supposedly WikiLeaks, which started taking and accepting Bitcoin. Then, we moved into the early days of Bitcoin specifically.

Around 2016, the big hype was blockchain, with the technology underpinning Bitcoin being usefully deployed in the commercial sector. This is when the birth of enterprise blockchain became a thing. It was very in vogue to go around saying, "The future isn't Bitcoin. It's blockchain." This is where a forking, so to speak, in the way the market perceived the technology came about.

Then we had two developments. We had the enterprise blockchain, which is how it is being applied and researched by very standard institutions from central banks to everyone—traders in the financial sector, and even commercial companies, everyday ones, retail ones, are looking at it.

Then you have had the public blockchains, which are mostly focused on the cryptocurrency side. Now, with Ethereum in the last few years, there has been this massive deployment of smart contracts, which have spawned their own derivatives and other blockchains as well based on other smart contracts.

Q12   **Carol Monaghan:** What is a smart contract?

Izabella Kaminska: In the blockchain world, if we go away from the enterprise, park the enterprise blockchain in one section because it is very different from the public blockchain. In the public blockchain, you have two types of blockchain. You have the standard cryptocurrency ones, which are like Bitcoin, and, as David was saying, they are either based on proof of stake or proof of work.

Then you also have the blockchains that are programmable, such as Ethereum. On Ethereum, you can house smart contracts and in theory those smart contracts can allow you to automate all sorts of transactions. The sky is the limit in how you can deploy these smart contracts.

What is a smart contract? A direct debit is a smart contract: anything that tells a program, "If this, then that." It can be almost anything. Currently, the very popular deployment of smart contracts is in this new realm of cryptocurrency called DeFi, decentralised finance. You might have heard about that recently because the entire sector is currently collapsing and causing massive headache and upset in the industry. Again, it was interesting you referenced 2008. I would argue the exact opposite of transparency has happened. We have ended up recreating all the mistakes that we never learned from in the first place in DeFi.

Q13   **Carol Monaghan:** Thank you. Mr Shrier, do you want to come in?

David Shrier: Yes, if I may. To amplify on what is exciting about smart contracts, our old style of working with data has been that data sits in one place and the code that tells the data what to do is somewhere else. Smart contracts put the code and the data more closely together. This means your data can travel around and have some intelligence around it. This can do things like helping to manage or distribute digital identity. Instead of trying to grab all your personal information from various places and use it for things like moving money or getting healthcare, all of that logic can sit with the data.

Q14   **Carol Monaghan:** Is there a danger with that?

David Shrier: If it is not programmed correctly, yes—but no more so than a conventional data system.

Q15   **Carol Monaghan:** Izabella, there is a lot of chat about blockchain. From what you are saying, it has been used extensively. Would you say that the uses of blockchain are happening more than the understanding of it?

Izabella Kaminska: I would say that it is not being used that much. In 2016-17, there was a lot of hype, especially in the enterprise blockchain

world. You saw a lot of companies, even conventional companies, coming to market saying, "We're not going to be juice companies any more; we're going to be blockchain companies." It was a crazy time where anyone sending out a press release saying they had pivoted into a blockchain-focused role would see their share price go up. It was a real case of FOMO if you were not doing blockchain.

In 2022, when we look back, what has come out of that hype? Almost nothing. From most of the pilots that were run, most of the trials in enterprise blockchain, I cannot think of a single successful deployment of blockchain in the enterprise blockchain world. Most of them have floundered; most of the companies have either ended up looking for more and more money or have demised entirely.

One of the most famous cases and one of the most hyped ones was the case of Digital Asset Holdings, which was the venture being brought to market by Blythe Masters. She was a former JP Morgan banker who created credit derivatives. Blythe Masters left and was quoted this year at a conference saying, "We need to teach companies that they do not always need a blockchain." That seemed to be her big learning episode from having fronted a blockchain company, which she has now left: most of the time, maybe you do not actually need a blockchain; a lot of the time you can do exactly the same with a centralised ledger.

The added security is a slightly misleading thing to woo prospective investors. The security enhancements are, arguably, that everything is a trade-off. It comes with a bit more security, but a lot more complexity. Sometimes if you add complexity and the distribution of the same accounts across so many different ledgers, even if it is on a proof of stake protocol, that is not going to be as efficient.

Trust is the most efficient system. Of course, trust can be abused, so there has to be a balance in the market. In a high-trust society, the application of blockchain is much less advisable than in a society that is low trust. You also have to consider the context of the society and economy that you are deploying these technologies in.

Q16   **Carol Monaghan:** Is there a great enough understanding of what blockchain is among the public and politicians? If not, what are the implications of this?

Izabella Kaminska: This is solely my subjective perception. I see it still as a bit of a buzzword and there is a lot of replication, echo and parroting of concepts that you hear in the industry. When I interview these people and ask, "Do you know what you're talking about?", 99% of the time they cannot explain to me how it works; they have just been told by some consultants that it is the next best thing and is the future. Nobody really understands why. That reminds me of all the manias in finance history.

Q17   **Carol Monaghan:** We are politicians and we are not going to have expertise in every new technology; we simply cannot. Is it a problem that

we do not fully understand or do not understand at all what blockchain is? Does there have to be a level of understanding? I do not know how drugs are developed, for example, but I do not need necessarily to know how that is done.

Izabella Kaminska: I would argue yes, because one of the problems of the industry is that they have created a system that prints its own money. If you create a system that prints its own money, it is very easy to corrupt people. So, there is no better way to sway.

How do you deal with that problem? Only through neutral independent researchers you can trust who are not going to be swayed by huge amounts of money. Unfortunately, the system has evolved in such a way that all the crypto press is either backed by crypto entities—there is very little free press—and the mainstream press has been either very positive or negative. It is hard to be neutral these days because crypto companies are coming in and trying to sponsor all your events. So, eventually you buckle and end up developing a specific crypto-focused desk. You have to cover this stuff, do not get me wrong, but everyone is under the influence because there is no convention.

Q18   **Carol Monaghan:** Is that why we have seen Bitcoin, for example, grow so much in value—because it is not backed by anything? Normal currency is backed by gold reserves, so there is not much substance behind that.

Izabella Kaminska: Arguably, real currency is not backed by gold. Without going down very complex financial architecture, Bitcoin is backed. The better way to say it is that fiat currency, conventional currency, is backed by the trust in Government and the Central Bank and the fact that the Government can tax everybody. If there is a deficit of capital in the system, you have the option to raise taxes and pull in more capital from the system.

Bitcoin does not have that central authority that can do that. What it does have is hackers who can extort money from you. I always say the value of Bitcoin is supported by the hackers, because ultimately if you have had your data stolen from a computer and there is a hacker claiming he will only release it if you give him Bitcoin, that creates the same underpinning value in crypto.

That said, I do not want to be entirely negative on the sector because I do think in low-trust societies you cannot trust your own Government because everything has collapsed—say, in Ukraine, or where there is war. Ukraine is a very good example where there has been a thriving cryptocurrency market evolving, because essentially they have to find a way to fund things.

The context really matters; the type of society that you are talking about. Given that you never know how society might go, having some sort of element of a cryptocurrency out there as a last resort is not a bad idea.

Should it be the go-to standard in finance? No, I definitely do not think that is the case.

Q19   **Carol Monaghan:** Thank you. You want to come in, David.

David Shrier: Just on a couple of points, if I may. I respectfully agree with my esteemed colleague's comments in some regards and disagree in others.

Most importantly, on the education point, I have dedicated quite some time over the last several years in educating Government officials about blockchain and cryptocurrencies. In my dialogue with organisations like the Bank of England and HMRC, there is already quite a bit of expertise in the UK Government around these technologies and around their application. The UK, in fact, is probably one of the five to 10 most sophisticated domiciles in the world around this subject.

So, I would not underestimate what is already here. I would argue strongly for more education, particularly among policymakers. I also want to make sure we do not lose sight of the fact that Bitcoin is only one kind of cryptocurrency, and cryptocurrency is only one application of blockchain. For example, the Government of Australia have collected tens of millions of Australian dollars in tax around, in this use case, liquor sales. It is very complicated, with lots of paperwork; they have simplified a lot of that at about 45 million Australian dollars of tax collection for a cost of 3 million Australian dollars—incremental tax collection.

The technology does solve problems. It is getting past what they call the Gartner hype cycle of all the exuberance and then despair. Now, we are getting into useful applications. Some of the work around managing the pandemic, for example, was supported by certain blockchain applications. Let us not forget blockchain is not just cryptocurrency.

Q20   **Chair:** We are looking at the interaction—questions of public policy as well as the technology—so it is important to be completely transparent. I introduced you both with your titles. Professor Shrier, you are a distinguished academic but you also advise companies and Governments; we should put that on the record.

David Shrier: Yes. I have a number of private sector interests that are all disclosed at visionaryfuture.com under portfolio.

Q21   **Chair:** Ms Kaminska?

Izabella Kaminska: I am currently self-funded.

Q22   **Chair:** It is important to be transparent.

May I delve into some of the technical aspects again? Ms Kaminska, you have talked about proof of stake and proof of work as being how entries are validated. Could you give as simple a guide to that as you can?

Izabella Kaminska: The proof of work uses this complex puzzle-solving system where lots of computers basically have to compete against each

other to solve a puzzle, a very complex algorithmic puzzle. The puzzle's complexity changes according to how many computers are trying to solve it, to ensure there is always a stable amount of supply. Whoever wins the puzzle gets a Bitcoin according to a pre-scheduled creation program.

That burns a lot of energy, and with more computers coming in to do it, there is competition with respect to the processors. We have seen a lot of capital invested in making these computers evermore efficient. What has also happened is that mining pools have evolved to try to draw even more capital. Now there are, effectively, large syndicates of computers that compete against other syndicates to win these coins.

It is quite funny—this is relevant, and I will move to proof of stake in a second—in the DeFi evolution of blockchain that these massive computer syndicates now have a lot of power. So, you end up with a situation as far as I understand—and I am sure the speakers who follow me might be able to offer some more insight—where they hold so much power over these networks that they can determine which transactions go into the blockchain and which ones do not.

This idea that it is entirely decentralised and there is no essential dictating authority is not true. The blockchain mining companies have a lot of sway. You can effectively pay them off to not put a transaction in if you do not want it; that is new financial innovation in the space. It is a type of front running, because everything in the blockchain is public and transparent, and, yes, that is very good on the one hand. However, if everyone knows what you are going to trade, they can also take advantage of that information and can jump ahead of you. If you can effectively bribe the miners to take your trade instead of other people's trades, you can front run them. That is what is happening with mining.

Proof of stake is supposedly more efficient because it does not rely on all these algorithmic puzzle-solving protocols. It is still distributing a lot of data across a lot of computers. So, if you compare it to a conventional centralised system, it is still less efficient than a centralised system. Yes, there are advantages with proof of stake and energy. But those advantages are also the vulnerabilities, and some might say that proof of stake is really beginning to emulate the older systems in finance, apart from the mass distribution. A central bank will also have back-up systems. It will not have them over thousands of computers, but it might have them over three or four. So, everyone has back-ups; that is essentially how you can think of it. Proof of stake is a ledger with many, many back-ups.

Q23   **Chair:** Thank you. On the proof of work front, why should your capacity to deploy vast amounts of computing power and to incur vast energy costs correlate with your ability to confer trust on a transaction or an enterprise?

Izabella Kaminska: If you think of it in conventional society terms, instead of having to pay off one corrupt cop, you have to pay off 10,000

corrupt cops to get them to change the ledger. You are essentially making it more expensive to corrupt the system, and that effectively means that only really, really powerful billionaires can do it, potentially.

Q24   **Chair:** Mr Shrier was nodding. Anything to add to that description?

David Shrier: To the point on disclosure, I am currently involved in a transaction engaged in one of the very large mining companies that compete to calculate Bitcoin. I agree with my colleague. It is not truly decentralised; it is an illusion. It is not truly anonymous; that is also an illusion. It is not magic. However, for certain use cases and applications, the fact that you have to apply all this computational power better secures the transaction.

Q25   **Aaron Bell:** I thank both of you. It is good to have such expertise and some healthy disagreement, because I think we learn more from sessions when witnesses do not just agree with each other throughout.

Mr Shrier, to carry on from where you left with Ms Monaghan, we have talked a lot about financial services. Can you outline some of the other ways in which blockchain has already been used, or could be used?

David Shrier: I will cite a few examples. First, in Papua New Guinea the Government were trying to drive societal inclusion around digital identity and secured a biometric identity using blockchain. In sub-Saharan Africa there is a company with an initiative called AgroTrust that is using blockchain to help open up the supply chain around areas such as food traceability—from field to fork; price transparency for farmers; certifications around issues like fair trade; and the use of fertiliser, pesticide, etc.

In the health area, a company called BurstIQ in the US is unlocking clinical research data using blockchain. One of the problems with the billions upon billions that we pour into clinical research is that, because of the privacy and protections around health data, if you are a patient in one of these trials it is dedicated to just that one trial. If 10 years later we want to use that data for a different drug, tracking down all those patients is impracticable. Blockchain can help to solve that problem and get a better return on that pharmaceutical investment. Those are just a few examples.

Q26   **Aaron Bell:** Do you think that any of those use cases have potential for the UK economy, or are a lot of them based on the fact that there is a lack of trust in some of these examples in the first place and the blockchain is trying to solve a lack of governmental trust?

David Shrier: That is part of it, but it is not only lack of trust. How lack of trust gets reflected is in things like the fact we use many intermediaries that we could replace with automation and technology. A number of applications in the UK economy include extending the UK's excellence in pharmaceutical and biomedical research; introducing greater efficiencies even in several areas of the UK Government like DWP,

where 20 million payment streams can be better and more efficiently managed with greater protections—certainly for the collection of tax; and the management of supply chain not just in food provenance but all areas of the supply chain. I think that you have the largest supply chain financial institution in the world housed here. Unlocking all that data can introduce greater efficiencies that will help businesses and the UK economy to be more competitive.

Q27 **Aaron Bell:** You mentioned the DWP. There have been quite a lot of suggestions about how the public sector could benefit from blockchain. Are there some cases where we could use distributed ledgers for public sector services, whether it is identity or personal records? Are there any ideas that could apply to the UK? What would that look like?

David Shrier: One of the examples is interrelated. Remember: blockchain is just one piece of the puzzle. What I find most interesting is when you use blockchain with other things like artificial intelligence or big data systems, but in the instance of DWP a lot of people who are on a fixed income or supplements are prey to payday lenders; they have to finance from payment to payment and they are struggling. We could help to introduce a better financial support system for those payment streams in concert with better distribution of the funds through the use of blockchain.

Q28 **Aaron Bell:** Currently, we are going through what is being described as a crypto crash. Paraphrasing what Ms Kaminska said earlier, there was a lot of hype and buzzwords and companies felt they needed to get involved because there was all this talk about it. The idea, bluntly, was that Bitcoin was going up and so on. Obviously, we do not know where the price of Bitcoin will be in six months' time, but has the crypto crash perhaps reduced people's willingness to embrace blockchain in non-financial or indeed financial settings?

David Shrier: Yes and no. It is important to remember that crashes are all relative. In the summer of 2020, Bitcoin was trading at about US$8,000; today, it is about US$20,000, so as an asset class it has performed well, if you got in in the summer of 2020.

I agree that it is speculative, as we alluded to earlier; it is not something I would recommend for the ordinary consumer, but, if you will pardon the expression, all of the hype and media attention around the headlines on Bitcoin in a way obscures some of the longer-term work that is going on in applications of blockchain in other areas, including central bank digital currencies.

Q29 **Aaron Bell:** Ms Kaminska, you probably remember that the Treasury Select Committee looked at this about four years ago. It published a report in September 2018 on crypto assets. One of its conclusions was that, although there might be some small-scale uses for blockchain, the Committee had "not been presented with any evidence to suggest that universal applications of the technology are currently reliably

operational." I think you said in your evidence earlier that you could not think of a single successful deployment of the enterprise blockchain. Do you think the conclusions of the Treasury Select Committee in 2018 still stand, or has the world moved on a little since then?

Izabella Kaminska: When it comes to enterprise blockchain, I would definitely agree with those conclusions. Blockchain is being used, but there is no definitive proof that it is being used in a better way than a conventional database. Where it is being deployed it is mostly so that the company in question can say it has blockchain, but whether it is or is not a better service is very much out there to be debated, even on the provenance side of things, which is a key use case potentially in the UK. People want to know where their food is coming from and that it has good provenance, but blockchain does not solve that problem because of the so-called garbage in, garbage out problem. Blockchain just records what you tell it to record, but unless there is somebody actually vetting the stuff getting into the blockchain—you have to spend money on trusted inspectors—it is meaningless. You are just snapshotting what is potentially corrupt or bad. It is like the horsemeat scandal. You do not know what is going on in the blockchain unless you check it, so I do not think that is necessarily a good example of it being deployed in a positive way.

Q30   **Aaron Bell:** You referred to garbage in, garbage out. One of the other problems with blockchain, as I understand it, is that you cannot delete anything that has ever gone in there. If something libellous has gone into a blockchain ledger there is no way to delete that, so there will be a permanent record of something. Obviously, you can also argue that it is difficult to delete something in the real world, but is that a potential problem with blockchain as well?

Izabella Kaminska: In the public blockchain area, that is one of the problems. That is why the institutional side, or the enterprise blockchain, has shied away from using public blockchains. They know mistakes happen and that often you have to resolve these things and change history, especially with financial transactions—fat finger trades or whatever.

That is why there is friction in the financial system to begin with: we have to do checks and figure out whether the money is clean or dirty. Some people will make mistakes. Massive enterprise blockchains have, as a result, shied away from the public, but at the same time they have recreated the old system. It is a paradox; it is an oxymoron in some ways. You either have everything transparent and out there or you have a central system. The enterprise stuff is a hotchpotch; it is a bit of both, and slowly it pivots back to a conventional system. They sell this as DLT, but is it really a DLT? Whether or not it is is very subjective.

Q31   **Aaron Bell:** Returning to cryptocurrencies and the report of the Treasury Select Committee, we all know that currencies have three purposes: store of value, a medium of exchange and a unit of account. That report

said that as yet there were no so-called cryptocurrencies that served all those functions. Is that still the case?

Izabella Kaminska: Pretty much, yes, especially now in the crypto crash. Stablecoin was an innovation that hoped to be some sort of medium of exchange potentially, but a lot of the Stablecoin infrastructure is centrally operated as well. Stablecoins themselves are not immune, as we are now learning, to runs and collapses. Therefore, I doubt they will be able to compete with a conventional currency that has a central bank standing behind it.

Q32   **Aaron Bell:** Finally on the crypto crash point, there is so much out there that has been designed essentially as scams. I hope *Hansard* will forgive me, but there are so-called shitcoins and NFTs. Is there any way for the sector to get away from the fact that it is becoming associated with scams and with ways of people pumping and dumping things, or is that inevitably part of any mania, which is essentially what we have been going through?

Izabella Kaminska: NFTs have grabbed the most headlines recently because we have had all these crazy Bored Apes being sold at record prices, but there is something interesting about NFTs. As a creator, there are some potentially interesting technological aspects that could withstand the crypto crash, but the law has not caught up with the technology. For NFTs to be deployable in a useful way, the copyright law has to sync with what the NFTs are doing, but copyright law and the law trump whatever the ledger says. In the crypto space, code is law, but in reality code is not law; law is law. If the two are harmonised and there is a connection between them, especially in the copyright world, there could be some interesting deployment, but we are nowhere near that. It would involve a lot of legal work.

Q33   **Aaron Bell:** Who should regulate that? We have an Online Safety Bill going through at the moment. It strikes me that some of this stuff is, to use the phrase, legal but harmful. Should the FCA get involved in things like NFTs? Should it be DCMS, or should there be some new regulator?

Izabella Kaminska: That is a good question. On the financial deployment side, the FCA is the obvious candidate, but on the NFT side you would have to think about it.

Q34   **Aaron Bell:** We have what happened with the Football Index, which I do not believe was a blockchain set-up. That basically fell into the gap between the Gambling Commission and the FCA, and the same sort of people are getting involved in these crypto scams.

Izabella Kaminska: There definitely needs to be some regulatory oversight. Perhaps a new agency might be a good idea. It will certainly not go away. Pandora's box is open and out there; it will continuously evolve.

One thing we have learned from crypto is its amazing propensity to reinvent itself and continue to come up with new terms for old concepts. That will continuously happen and every new generation will continue to fall for it. There should be some kind of regulatory body that looks at these things. I am inclined to say it should be the FCA, but I do not know.

David Shrier: The industry has a PR problem more than anything. I note that the former head of blockchain for the World Economic Forum, Sheila Warren, is helping to organise a number of the prominent cryptocurrency companies better to engage with the public and Government around what the industry is and is not doing.

I note that it is getting increasingly institutional. State Street, the largest custodian in the world, has gone into the crypto space with a company in which I have some involvement.

The FCA is probably best constituted among the current Government bodies, but, whether it is the FCA or you extend the regulatory perimeter of another existing agency or body, I do not think you need a new distinct agency.

Finally, I would direct you to look at the example of what Bermuda has been doing, first with the digital assets currency Act and, more recently, with the setting up of the first new bank in that country in 50 years that is built around blockchain and is now announcing its own central bank digital currency. Bermuda is an interesting example to look at from a policy and public-private partnership standpoint.

Aaron Bell: You might have anticipated the next questions.

Q35   **Chair:** Indeed. Ms Kaminska, before I turn to my colleague Chris Clarkson, who has some questions about regulation, you had a discussion with Mr Bell about non-fungible tokens. Were you surprised that the Treasury instructed the Royal Mint to issue NFTs during this year?

Izabella Kaminska: It did catch my eye. Everyone is doing it. It would be negligent not to get in on a potential revenue-generating activity. There is a market for it. Galleries are looking at it; historic art is being put on NFTs. The question I would pose to the Treasury Committee is whether it is a good idea to encourage it.

Q36   **Chair:** There are a few aspects. The Treasury is the sponsor department for the FCA and a number of other regulators. You have given evidence to us that there is not an adequate regulatory system there at the moment, and presumably the Treasury would know that.

The second thing is that some people might regard the Treasury's involvement and instruction as amounting to some kind of encouragement.

Izabella Kaminska: I think it is, but the fact that it is the Treasury doing it is very significant. The Treasury is the Treasury and it is de facto

issuing it via the Royal Mint NFTs. In a way, it is issuing its own additional money directly outside the central bank. It is arguable, but in the US there is a proposition for the US Treasury to start issuing its own digital money directly to compete with the Federal Reserve on a CBDC-type platform.

These ideas are out there, but it would be interesting if the Treasury NFTs ended up competing with the conventional central bank money and circulating it as their own. You would have a money civil war here in the UK. It is hypothetical, but I presume there are only a few. I am sure there are not enough Treasury NFTs out there.

Q37   **Chair:** You referred earlier to FOMO, which is fear of missing out. Do you think that is driving the Treasury's interest?

Izabella Kaminska: Potentially, yes. I am not in the Treasury and I do not know what it is motivated by, but it seems to be a kind of gimmick that is mostly for headlines. At the end of the day, it is a collectible. If that collectible in a crisis becomes a medium of exchange, that would be quite an interesting economic thing to watch. Whether it would depends on how many of those NFTs there are, but, if the Treasury proves itself able to manage that process, in theory it could start issuing its own money via NFTs. Effectively, we would be nationalising the central bank in that sense.

Q38   **Chris Clarkson:** Professor Shrier, you mentioned a few countries that have been fairly proactive in their use of blockchain and distributed ledger technology: Australia, Papua New Guinea and a new bank in Bermuda. Are there any others that you would flag up as being particularly proactive? What I am interested in is what lessons we can learn from how they have applied it. Are there some things here on which we are missing out?

David Shrier: There are lessons that are both positive and cautionary. Canada, Switzerland and Singapore are three other domiciles I would call out as worth looking at. I also know that the OECD, for the first time, got together a harmonised policy recommendation around blockchain. I do recommend reviewing that. It distils a lot of lessons into one helpful guidepost for government officials.

Do not be New York State. New York City managed to blow up its potential leadership in fintech and blockchain several years ago by putting the wrong kind of regulation in place. It was something called bit licence. It was an effort to control all this innovative activity, but it basically created an economic barrier to starting new companies that amounted to hundreds of thousands of dollars. Effectively, it said, "We are giving up, and London and other centres of financial innovation and excellence will pioneer this new world." It has been very difficult for New York to come back from that.

The UK has several advantages over countries like the US because of the consistency and centralisation of its regulatory activity in areas like the financial system. By my last count, the US has at least 100 different government offices trying to manage or regulate Bitcoin cryptocurrency, and blockchain has created massive confusion.

You do not have that, so the UK has a potential competitive advantage. That competitive advantage is important. Let us not forget that China, for example, is very aggressively pushing forward with a central bank-sponsored digital currency and is looking to go beyond mainland China into the entire region and globally, using this to architect a financial system that it controls.

This is a complex geopolitical landscape and the UK has a role to play. The UK has certain advantages because of its excellence in financial innovation, and regulation can help to support that competitiveness while protecting consumers and managing systemic stability.

Q39 **Chris Clarkson:** When we talk about regulation, how light touch should that be? You have given the example of a bit licence. That sounds quite heavy-handed—it is paying for access to the market. Are we talking about something like the FCA but for crypto? Are we talking about giving management of crypto to the FCA?

David Shrier: I think that policymakers providing greater clarity and guidance for the implementing departments and bodies would be helpful. I want to be thoughtful in my response because I do have some commercial entanglements. For example, I am a non-exec director of one of the three FCA-licensed wallets in this country: it is a company called Mode.

That is a clear example of where the system is working: clear guidelines are provided to entrepreneurs and entrepreneurs are engaged in compliance. The Government now have an innovation that is still within the regulatory perimeter of an existing and very experienced body.

I want to emphasise the importance of providing clarity. That is what good policy regulation can do. Right now, we still have some grey areas here in the UK.

Q40 **Chris Clarkson:** Obviously, we as policymakers will have to consider this. What are the key questions that we ought to be asking? Is there any one in particular that we think we need to be drilling down on?

David Shrier: Let us call it 80/20. Eighty per cent. of where policy can go—yes, the Pareto principle—is towards better supporting innovation and the UK's competitiveness in areas like fintech and blockchain, because we are already starting to see unicorn companies starting to leave UK-focused business activity and move to more friendly domiciles like Switzerland. That is bad for the UK.

I believe it is important to support consumer education and education of Government officials to help engage in that dimension of consumer protection. That can be supported through, for example, tax on the industry or other revenue-generating activities related to the industry, so it can be self-funding.

More education is important, but I think regulatory clarity around what is and is not acceptable business activity for cryptocurrency companies would probably be the No. 1 thing that would help to prevent this flight of intellect and capital from London.

Izabella Kaminska: On the regulatory point, consumers need to be protected. One of the biggest areas of concern in my mind is the celebrity-endorsement side that you see across Twitter and all the social media spaces. That is one of the key mechanisms by which unsophisticated investors enter the space. I guess that might be an issue for advertising standards. I am not sure about the particular regulator.

On the financial side, I would consider that the key question is whether, if we go too heavy on it, everyone will move to Switzerland. Is that a problem? Do we mind if Switzerland takes them all? I do not know. Maybe not having that volatility here in the UK would be a good thing, so I am not necessarily sure that is the case.

As I said earlier, I am not entirely negative about the sector. There is a positive role for something like Bitcoin in the sense that people are losing trust in institutions across the entire world; there is a general distrust because of disinformation, etc. Bitcoin provides a competition to central banks, and if we can create an environment where there is a concordat between the two the public will benefit from knowing that if the central banks go wrong there is Bitcoin.

In an optimal situation Bitcoin is there, but never used. It is like a last-resort currency that can add confidence to the core system because you know there is a plan B, if there needs to be one, but optimally it just keeps the core system honest and secure, because the institutions know that, à la Switzerland situation, if they do not measure up to their own standards people will flee to Bitcoin.

It is a good mechanism to keep the core system honest, and from that perspective you should not do a China and completely regulate Bitcoin out of existence. I think its existence is useful, but maybe on an institutional or wholesale collateral basis—sophisticated investors only sort of thing. That would be my preferred perspective, but it is a debate.

Q41 **Chris Clarkson:** Almost like a holographic reserve currency.

Izabella Kaminska: This is a cliché, but in America you have the right to bear arms and the justification for it is always that if the Government go wrong people will have their own arms. In that sense, it is the financial equivalent. To some degree, if it is out there that is great; it will

keep the core central banks and banks, hopefully, honest, but you do not want to use it. Ideally, it is there but you never have to go there.

Q42 **Chris Clarkson:** I am not entirely sure you can use the second amendment as a reason to do anything.

Izabella Kaminska: It is not optimal, but the "last resort" idea is what I am trying to say.

Q43 **Chris Clarkson:** In case of emergency, break the glass.

Izabella Kaminska: Yes.

Chair: I thank our two witnesses, Mr Shrier and Ms Kaminska. You have introduced a very technical subject with great clarity and have helped us in this morning's inquiry. Thank you very much indeed.

Examination of witnesses

Witnesses: Dr Robinson and David Gerard.

Q44 **Chair:** I now invite the next pair of witnesses to join us at the table. David Gerard is a journalist and author. He writes the cryptocurrency and blockchain news site, "Attack of the 50 Foot Blockchain".

I am also pleased to welcome Dr Tom Robinson, chief scientist and co-founder of Elliptic, which is a company that provides services to businesses, including crypto businesses, and regulators to help to detect and prevent financial crime in crypto assets, among other things.

Dr Robinson, it is clear that you have commercial interests. Mr Gerard, for transparency, as in the previous session, do you have any commercial interests as well as writing about these matters?

David Gerard: I have no interest in any blockchain or cryptocurrency company or product whatsoever.

Q45 **Chair:** To start with a question to you, Mr Gerard, it is perhaps implicit in your answer that you are something of a blockchain sceptic. Can you briefly outline the case against it, or perhaps the case for caution in the face of some of the opportunities and innovations we have heard about this morning?

David Gerard: The trouble with blockchain and cryptocurrencies, which are absolutely intertwined, is that there are people who argue that blockchain is completely distinct from cryptocurrency. Historically, that is completely inaccurate. Even today, it is promoted by the same people in the same venues using the same slogans. This discussion has been about both, intertwined.

The trouble is that it is full of promises that will always happen in a fabulous future: "It has not happened yet. It is early days; it will definitely be good soon; get in early while you can." It has been going on for 13 years and you would expect more to show by now.

Consider other technologies that came to prominence around the same time—for example, the iPhone. If we were sitting here 13 years later thinking, "I wonder whether anyone will think of a really good use for an iPhone," it would not be convincing.

There is a real air of, "It's early days yet." There have been lots of projects over the past several years and they have not really gone anywhere. There have been no really convincing use cases. I asked a lot of people in preparation for this, "Give me your best shot. What is the really convincing use case I can take along and I can say what's good?" It was all very vague. The most impassioned one was, "It's a use case because it gets venture capital funding." That is a use case. On the other hand, that was also the use case for Theranos, where medical fraud to get venture capital funding makes money but has a number of other problems.

Q46   **Chair:** What are the mooted use cases that were put forward and have foundered?

David Gerard: Many of the ones you have heard about. For example, supply chain cases all tend to be pilot programmes or funded by large amounts of venture capital, but they are not successful industries and so on. I think the most prominent were two put together by IBM. They were very full on with their blockchain units from 2015 to 2019 or 2020, when they shut it down. They managed to sell systems, which I think were vendor-funded trials—I am not sure and would have to verify that—to Walmart and Maersk, the largest shipping company. These were sold as having many advantages of blockchain where you have a ledger that records data that cannot be altered. That is good.

The other problem is: how do you know that the data is good? It turns out that crooks will fake data digitally as well as on paper, and ultimately your problem with supply chains is not having something written down; it is that human frauds are creative. I have spoken to people who work in supply chains and asked, "Why didn't you buy a blockchain product?" The answer was, "Because it doesn't do anything for us."

The answer to supply chain problems is that you need human inspectors who know the industry and the scams; they can go out and meet the supplier and say, "Show us your factory," or whatever.

Blockchain provides security of bits that are not an actual problem and do not need securing. A lot of the claimed innovations take something that does not need a blockchain and think, "Can we apply a blockchain to this? Have we applied a blockchain to this?" They start from the technology and then say that is the solution.

We use the word "technology" a lot. A blockchain is very simple technologically. It has an air of mystery about it and people say, "Oh, it's the technology." I think a lot of this is because people do not know what it is or do not understand it, or when you tell them what it is they say,

"That's too simple; that would mean this thing is completely stupid. I must be misunderstanding it."

The technology is simple. If you have an accounting ledger you can add new entries to it; you cannot cross out old entries. It is a digital version of that. Then you have a mechanism to decide who gets to add new entries. That is more or less a cryptocurrency blockchain.

Enterprise blockchains have some components of this. The words "blockchain" and "enterprise" are often marketing terms. Many of these products are not even a blockchain in that sense, but they are marketed as a blockchain and used as evidence of a blockchain revolution.

Q47   **Chair:** To take an example of a supply chain, suppose that you are, as we are in this country, building a new nuclear power station and you want to be very sure that every component is absolutely what it is purported to be and is reliable. If you take a component that has been sourced from somewhere else, might you think of blockchain as an absolutely impregnable guarantor of its provenance and something inferior has not been smuggled in? Might that be an example where blockchain does not add anything in your view to the systems that have to take place?

David Gerard: The problem with things like that is that, first, it is basically a method of tracking data in a ledger from which you cannot remove things. The point where supply chain use cases really fall down is that there is no intrinsic link between the entry on the ledger and the object. I remember there was a mooted plan with HS2 to track every bolt. How are they going to do that? Are you going to go out to the railway line and scan the bolts' QR codes and check it on the blockchain? Probably not.

There is also a tendency in blockchain promotion to say things that are hypothetical, or are coming in the future, as if they are in the present tense, such as "blockchain could," "blockchain might," "in the future blockchain will," or "definitely in six months we will do such and such." All of these are ways of saying that it does not do it. "Could" is a word for "doesn't". That is very important.

By day, I work as a system administrator in IT, so I know technology. This is not complicated technology at all, but I think it has one of the highest ratios of hype to production systems I have ever seen in any technology of any sort. I have seen quite a few hype waves—for example NoSQL, the cloud and so on. These were very hyped and there were lots of failures, but there was an actual technology there. Here, I am not entirely convinced.

Chair: That is evident.

Q48   **Aaron Bell:** Dr Robinson, it is nice to meet you and Mr Gerard. Can you briefly introduce your firm, Elliptic, and outline what part you play in the

ecosystem and how you use blockchain technology yourselves?

Dr Robinson: At Elliptic, we provide software and services that help to prevent crypto assets from being abused by criminals. One of the best analogies for Bitcoin and other cryptocurrencies is that they are digital cash, in that, like cash, they are bearer instruments and do not need to be held in an account with a financial institution tied to an identity.

Therefore, Bitcoin and cryptocurrencies can be useful tools for criminals in the same way that physical cash is. For example, we have seen Bitcoin and other cryptocurrencies be the payment method of choice for ransomware operators, dark net market operators and so on.

However, those risks can be managed. A lot of this criminal use of crypto can be identified and tracked because of the inherent transparency of blockchains. If you think about Bitcoin, for example, every single transaction that has ever taken place is recorded on that blockchain. You can see the details of the transaction, the sending and receiving wallet and so on.

What you do not have is any concept of identity. A wallet is identified by a string of letters and numbers. Companies like Elliptic do research that enables us to link some of those wallets to known entities, such as dark net markets, legitimate exchanges or custodians. That basically provides a map of each blockchain. What it means is that a regulated financial institution, such as an exchange, can screen a cryptocurrency deposit from one of its customers with our software and identify whether it has originated from illicit activity like a dark net marketplace. Therefore, it helps them to meet their anti-money laundering obligations.

Our services are also used by regulators and law enforcement agencies. If a law enforcement investigator is investigating some kind of criminal activity involving a cryptocurrency and they have the wallets being used by the criminal they can follow the money using these blockchain analytics tools, usually to the point where the crypto has been cashed out through an exchange. Those exchanges generally identify all of their customers, so it allows law enforcement to tie the criminal activity to a real-world identity.

This is highly effective. What we hear from law enforcement investigators is that they like it when they see a criminal using crypto because it is easier to follow the money and identify who is behind it than if they use physical cash, which is far less traceable.

Q49   **Aaron Bell:** That is all very well if the hacker or criminal is within reach of law enforcement and is not in Russia, China or somewhere like that.

Dr Robinson: Yes, absolutely. Having said that, a lot of the pools of liquidity when it comes to crypto are in places like the United States. If a Russian cyber-criminal is looking to cash out a large amount of cryptocurrency they will probably have to go through one of those liquidity pools outside Russia.

Q50   **Aaron Bell:** It is obviously good that there is a company like yours trying to clean up this space. I know you were listening to the previous session. I was very struck by what Ms Kaminska said. She said that essentially the hackers, or the speculative bubble in there, were the people who supplied the need for liquidity in the first place. They are taking on the role of the state in taxation; the hackers are essentially taxing the ecosystem of bitcoin. Is that something you recognise?

Dr Robinson: Responding to David's comments in general, I established a blockchain company, which I work for. I have been working in this industry for nearly a decade. I agree with most of what David said.

Part of the issue here is that blockchain is a term that encompasses a wide range of different technologies and use cases. In particular, it is useful to make a distinction between enterprise blockchain and open public blockchains like Bitcoin. In about 2015 a narrative emerged that basically said, "Cryptocurrencies are just used by criminals, but the blockchain is interesting, so we will try to take away the anonymity and openness of Bitcoin and see what is left over and whether we can make anything out of it."

I think the learning over the past five to six years is that enterprise blockchain has not really succeeded. It is trying to apply technology that was designed for a specific operating environment to something very different.

Contrast that with cryptocurrencies. DeFi has grown exponentially. There are tens of billions of dollars' worth of transactions every day. Over 50% of all financial institutional investors now have cryptocurrencies as part of their portfolios, so it is important to recognise crypto assets as a distinct part of blockchain, which has seen considerable success.

Q51   **Aaron Bell:** Therefore, you are negative on the enterprise blockchain but, given your business, quite positive on the financial services sector. Are there any other uses of blockchain that you think are particularly unique or beneficial?

Dr Robinson: What is interesting about this space is that I do not know how blockchain will be applied next. What drew me to this technology is that it is a fantastic open platform for innovation in financial services.

A useful analogy is with the internet. I think we are at the early '90s stage, if we try to make that analogy, in that there is growing recognition that this is a fantastic platform for innovation. The actual use cases are very early stage or somewhat nebulous at the moment.

Q52   **Aaron Bell:** You mentioned that a lot of people are getting invested in blockchain or crypto assets. What risks would you highlight for those individual institutional users and investors? People say they are aware of the risks, but do you think they really understand them?

Dr Robinson: I do not think so. Everything within the crypto space today is still an experiment, even something like Bitcoin which has been around for over a decade. Sometimes investors do not appreciate that. It does not necessarily mean that it is a bad investment, but investors need to have a proper appreciation of the risk.

Q53 **Aaron Bell:** Looking at the recent crypto crash, your firm does a lot of work with Coinbase in particular. You advertise that on your home page and so on. It is a crypto brokerage and exchange. Its shares are down three quarters this year already. Goldman Sachs issued a rare sell on Monday. How concerned are you about the crypto crash, not specifically for the wellbeing of your business but the whole ecosystem, or, as we discussed in the first session, is it a crash that will probably bounce back again?

Dr Robinson: This must be the fourth or fifth crypto crash through which I have operated.

Q54 **Aaron Bell:** You should plot them on a log scale, a bit like Covid.

Dr Robinson: Absolutely. Each crash results in crypto prices that are still larger than the price in the previous market cycle.

Q55 **Aaron Bell:** You are still bullish overall?

Dr Robinson: I am still bullish overall. However, these assets are highly volatile. The market still has not been able to decide what they are worth; there is still a big variance in the value different people put on these assets, and therefore it results in a lot of volatility.

Q56 **Aaron Bell:** Mr Gerard, what do you think of the implications of the current crypto crash for the ecosystem and for us as policymakers?

David Gerard: Forget about the technology bit because that does not matter. In that case, it is just blockchain as a sort of excuse. It is not even a technology enabler; it is really an excuse to create a whole world of financial assets of varying degrees of regulation, some of which evade regulation by saying, "Oh, we're a blockchain." What is a blockchain?" It's technology." "Oh, that's all right then."

I think it is not all right then. Ignore the technology; treat them as the financial assets they look like. It is good that we have companies like Elliptic and other competitors like Chainalysis, or whatever, which do the compliance stage. If we are to have these financial instruments, we need proper compliance companies. That is excellent work, so that is good.

We have had the recent crash. A lot of it happened because of lots of leveraged bits in the DeFi space, which is basically a way of doing a wild and frantic forex market or derivatives of derivatives market, very like 2008. Crypto has done a small 2008 to itself in an isolated sandbox where we can just watch it happening without contagion to the rest of the economy, which is a very instructive example.

All of this stuff was visible on a blockchain. You could see people taking up outlandish positions and doing things that made no financial sense. It turns out that having all of this complete transparency made no difference, because the siren call of "number go up" blocked out all other considerations like risk and everything exploding, very like the lead-up to 2008.

Q57   **Aaron Bell:** You said there is no wider contagion. From a policymaker's perspective, is our biggest responsibility to end users?

David Gerard: What we have seen in crypto is that they have tried very hard. For example, no one treats cryptocurrency as money; it is just an asset you can buy yourself. If your goal is actual dollars at the other end—because everyone in crypto works in dollars—all you can do is sell some bitcoins or Ether.

Some of the Bitcoin miners in the US, particularly in the past year, instead of selling fresh bitcoins the moment they were created, they stockpiled them and borrowed cash against them. This had the effect of not depressing the Bitcoin market, which by the way is a very thin market. It does not take much to drop the price of Bitcoin. Unfortunately, it turns out that their lenders were other crypto companies and they are running out of cash, so a lot of miners are having to dump their coins, which is not helping the sell pressure.

Having this transparency has not helped at all, because no one listens to the risk; they just listen to the number going up. When someone believes that 5%, 10% or 20% is an achievable interest rate in this economy, what can you tell them? They are not listening to the risk; they just see the number and say, "I'm going to put everything into that." Retail investors are the victims: mums and dads go on morning television to say, "All my money has gone." It is box office poison.

Q58   **Tracey Crouch:** Some of this is blowing my tiny little mind, so I hope you will forgive me for reaching for my comfort blanket of sport. We have seen an explosion of cryptocurrency in this country, specifically and rather worryingly in football. Yesterday, Joey D'Urso in *The Athletic* noted that 19 out of 20 Premier League clubs now have a formal crypto relationship. Are you concerned by this? Do you think this is worrying?

David Gerard: I must commend Joey D'Urso's work at *The Athletic.* He has been covering this for the past year and has done a fantastic job. If you are concerned about this, read everything he writes about it; he is really on the ball with the crypto problem, which is basically that large companies with a lot of money are trying to buy a bit of respectability and an audience.

Sports clubs, even at the top level, are always strapped for cash; everyone is looking for a sponsorship. Second-tier sports teams in any sport are desperate for money and sponsorship. They will sign up with almost anyone. Sometimes these companies disappear. I believe that one

team—maybe Chelsea, but I need to verify that—got a shirt sponsor which went broke shortly afterwards and disappeared. I would not really blame the teams because they want cash and these companies are offering lots and lots of money. Are they going to say no? These companies exist.

Q59   **Tracey Crouch:** Given the volatility that you have spoken about and we have heard about in terms of cryptocurrency and crypto cash and the volatility in football finance, surely this will create the perfect storm or disaster of which the fans of those clubs, who are buying NFTs, for example, will be the victims.

David Gerard: The fans end up being the victims in this financial issue; they are the public interest here.

Q60   **Tracey Crouch:** The FCA said very clearly that if you buy crypto assets you should be prepared to lose all the money you invest, whereas we have seen sports people launch NFTs with claims that they cannot lose their initial value. Who is right?

David Gerard: I think the FCA is right because the ASA stamped down on that example. It turns out that the ASA, the advertising self-regulator, has been one of the most effective crypto regulators in the UK because it tells people, "No, you cannot advertise rubbish to ordinary members of the public." That has been quite effective. If people want to go out and spend their money on magic beans you cannot really stop them; maybe you should not be able to stop them completely, but you are certainly not obliged to make it easy, because a lot of crypto companies are perfectly decent people, but there are also lots of predators. They are not just offering an opportunity; they are predatory and deserve to be treated as such.

I have said previously I would love it if crypto marketing to the public was at least as regulated as gambling. That would be an improvement. At the institutional level, if someone has a trader—a well-off person, a sophisticated or high net-worth individual—their money is their own problem. We can talk about the details of how the market works and so on. On the other hand, in retail they are people where all the money in crypto comes from and they need more protection.

Dr Robinson: There is clearly a consumer protection issue in crypto. I think the root cause of it is that crypto technology can be very difficult to understand. It is a very complex topic. Couple that with the fact that early adopters of crypto have made a lot of money, so in that kind of environment it can be easy to attract retail investors who perhaps should not be investing in an asset class such as this. I think the solution to that is controls on promotions around crypto assets—I believe there is legislation on the way around that—perhaps controls around which crypto assets are made available by exchanges and education of retail investors such that they understand what they are getting themselves into.

Q61   **Tracey Crouch:** When you have celebrities launching NFTs clearly there is a risk of people being brought in by the endorsement. Mr Gerard, did you refer to that earlier?

David Gerard: I did not refer to endorsements; I think Ms Kaminska referred to it.

Q62   **Tracey Crouch:** I am sorry to be a one-trick pony here in referring to NFTs and football, but what do you think is the life span of an NFT in football?

David Gerard: About 10 seconds. The NFT market is very interesting because it was promoted into existence. The famous JPEG picture by Beeple that sold for $69 million last year was not quite a wash trade, where you buy an asset from yourself to make it look like you are driving up the price, but it was pretty close. The buyer, MetaKovan, had been working on a deal with the artist, Beeple, to package his pictures as NFTs and market a crypto token backed by the NFTs.

They were already very closely in business together. It was not technically a wash trade, but it certainly smelt a bit involved. I looked at that as basically a payment to Christie's of $9 million to get their name in all the mainstream press, and Beeple now has a Wikipedia page.

The NFT market had largely collapsed by April of last year. Bloomberg ran my favourite headline of all the NFTs; it called it "a stimulus-led fad", which is the politest way I have ever heard someone describe a market as completely fake. There is a lot of money in the US that is desperate for a home and a return. They are buying lottery tickets now; they are investing in weird nonsense in the hope that something will take off.

They got heavily into promoting NFTs and Web3, whatever that is. It is a meaningless promotional term. It was very seller-driven. There was no sign of a real public upswell. NFTs were promoted through everything: music, art and celebrities going on TV to talk about their fabulous new picture of an ape.

There is no evidence of public interest. The actual market is crypto speculators, who are always looking for new assets on which to speculate, because these guys love their trading and losing money. The public do not really like it much.

Video game companies and other companies got into this. Who can resist the call of free money? "We do NFTs; it's money for old rope," but the public hate it. I believe that the video game company Ubisoft did an NFT. With huge fanfare and lots of promotion, it eventually sold $396-worth and shut down the scheme.

On the earlier question about the Royal Mint NFT, the purpose was to get people talking about the crypto initiative. Maybe someone will buy the NFT at some point. I am not sure that the NFT was really the point there, but in the field of sport they are trying to sell collectables to fans. The

fans are not that interested. Some crypto speculators are, and obviously they are being paid by the companies sponsoring this stuff. It is a celebrity endorsement deal. Celebrities do endorsements, but you have to apply caution to what they say when they do that. Celebrities usually do not want to sell awful things to their fans.

Q63   **Tracey Crouch:** Dr Robinson, from a compliance perspective I am interested in your thoughts around regulation of NFTs and this particular product. For most financial products, if you were to switch a deal you would have some transparency and would know exactly what was going to happen to it, whereas if you take an NFT deal within a football club there tends to be a fixed period of time for that deal. When that deal is ended they can take out a new deal with a different provider. What happens to the previous asset that you, the consumer, have bought? The regulation seems very immature. I wonder whether you have any thoughts on that.

Dr Robinson: I am not familiar with that particular product, but fundamentally the issue is whether these are being sold as collectables or as an investment. If they are being sold as an investment with the expectation that they will increase in price, the promotion of that product needs to be well regulated.

Q64   **Tracey Crouch:** The collectability aspect is based on sentiment, is it not?

Dr Robinson: It is the same with something like a commemorative coin or any other kind of collectable.

Q65   **Tracey Crouch:** Presumably, the sentiment towards a football player or digital asset changes over time. For example, as a Tottenham fan, Sol Campbell was once upon a time very important and had great sentimental value. As soon as he was sold to Arsenal, that sentiment changed. Surely, the collectability of that asset—we use the word "volatile"—changes very quickly.

Dr Robinson: Yes, but I am not sure that has anything to do with blockchain. The same could be said of any collectable.

David Gerard: Like I said, ignore the technology bit. Take out the word "blockchain". Look at the asset. Look at what it does. Look at the people and the flows of cash. I say this all the time. Ignore all technology claims. The technology does not matter. These are financial assets. Treat them as financial assets. Look at how they are behaving, the people and the flows of cash, like you would any other financial asset.

A letter from assorted technologists—I was one who signed it—to the US Senate recently begged them, "Please, with the blockchain regulation, do not accept the word technology as an excuse." If someone has something that appears to be a really shonky scheme that is already banned or highly regulated, saying the words "blockchain" and "innovation" are not excuses. It is a balance. If someone is really innovating with finance, they do not need to say the word "blockchain"; they can say, "Look, we have

this scheme. Here are the plans. We think this will work." If it does not make sense without the word "blockchain", it does not make sense.

Dr Robinson: I differ with that slightly. There is a fundamental difference with blockchain-based financial services in terms of their level of decentralisation—there are generally fewer intermediaries intermediating transactions—and, secondly, their level of transparency.

David Gerard: They work differently.

Dr Robinson: If they are in a blockchain, every single transaction is visible, and that changes how you should regulate that kind of system.

Tracey Crouch: Thank you.

Q66 **Carol Monaghan:** Dr Robinson, are there any limitations of blockchain that you could highlight to us?

Dr Robinson: Yes, absolutely. Like any technology, it has its limitations. One of the key ones at the moment that is being worked on is scalability. If we think about Bitcoin, it currently has an inherent limit of about seven transactions per second, which obviously is not—

Q67 **Carol Monaghan:** Why is that? Is that because of the number of parts?

Dr Robinson: There is a trade-off between scalability, security and decentralisation. Bitcoin has really been optimised to be highly secure but also highly decentralised, and the trade-off there is you reduce the scalability and throughput of the system. Other blockchains have made different trade-offs and so are more scalable and have higher throughput but are more centralised and maybe slightly less secure.

Scalability is a big one, although there is a lot of work currently going on on new technologies that will improve the throughput of these systems.

Another big challenge at the moment is energy usage. Most blockchains at the moment use proof of work as a consensus mechanism, and that expends a large amount of energy. As was discussed by the previous witnesses, there is a move to shift to other consensus mechanisms such as proof of stake, which use a tiny fraction of the energy that proof of work does.

Q68 **Carol Monaghan:** I believe that some research done by the University of Cambridge shows that for Bitcoin alone the energy consumed is comparable to that used by a small country. Should that form part of a regulation process?

Dr Robinson: A lot of the benefits of blockchain come from the fact that the protocol itself is unregulated and there is no control over the transaction validators, which makes it an open system that anybody can innovate and build on top of. As soon as you start regulating at the protocol level, you sacrifice some of that.

Having said that, there might be an argument to be made that you could compel miners to use renewable sources. In fact, that might stimulate investment in renewable energy if all miners are compelled to use it.

Q69 **Carol Monaghan:** Mr Gerard, your scepticism is quite clear today. Do you foresee any situation that might cause you to change your position on blockchain?

David Gerard: Cryptocurrencies have a ton of problems. One of them is using up a country's worth of energy for the most inefficient payment system in human history, but there are moves to alleviate this, and, hopefully, they will eventually get them out. They have been trying for several years on one side. I know these guys. They are very sincere about it, but they have taken a long time to try to get it to work.

Basically, cryptocurrencies should be regulated as a series of financial instruments. Look at how the nuts and bolts of it work. As Tom said, that is quite correct. The details matter, but, first, approach it as a financial instrument.

In terms of the blockchain itself for enterprise, speaking with my system administrator hat on, one of the things I do is look at new technologies and ask, "Is this technology any good? Is it better than what we have?" So far, it has not been better. I will not say it will not in the future. Fundamentally, if you control the system, it is a form of data store. It is just a database architecture. That is getting very detailed. A database architecture is not magic. It does not create trust.

Blockchain in the sense of the word "trust" is a very specific jargon term in terms of mathematically how one computer can trust another. It absolutely is not the general squishy English word "trust", but it gets used that way, and that is not quite correct. Trust is always in a given situation with given parameters.

It is just a data store run by an organisation. Maybe it will help the organisation to co-ordinate—fine. I know of blockchain deployments.

Q70 **Carol Monaghan:** Are you open-minded enough? Are you against blockchain for the sake of being against it because of your background in software, or are you open-minded enough to say there may come a time where—

David Gerard: If you show me a system that is a convincing case, I will look at it and be convinced. There are existing systems that have blockchains and do useful jobs. I would not have chosen that as the architecture, but I would not say, "Rip it out," because it is a working system.

Q71 **Carol Monaghan:** Okay. So, we should watch for your comments on this in the future to see whether you change your position on anything.

David Gerard: I have been looking very closely for years now and saying, "Does this do the job? No." It has been sadly disappointing. Prove me wrong.

Q72   **Carol Monaghan:** I do not think it will be for me to prove you wrong.

David Gerard: That is what I mean. I want to be shown wrong on this.

Dr Robinson: I just want to call out one point David made on the technologies to reduce the energy consumption of blockchains. They already exist and they are being used. Some blockchains already use proof of stake, which uses a tiny fraction of the power of proof of work.

He is right. Ethereum, one of the larger blockchains, has been working for a while now to move to proof of stake, but it has been successfully deployed in other blockchains.

David Gerard: Yes, that is true.

Q73   **Carol Monaghan:** I have a final question on the energy aspect. Do you think it is understood enough by the public and politicians how much energy is consumed by cryptocurrencies?

Dr Robinson: It is rising to the top of the agenda. We have seen in the US some legislation to ban crypto mining in some areas. Yes, there is a growing awareness of it. However, I do not think there is enough awareness of the technological solutions to this issue.

Q74   **Chris Clarkson:** Could you suggest one priority for the UK Government when thinking about blockchain?

David Gerard: Financial regulation and protection of consumers. For the UK, that is the big one. Crypto mining is not really relevant to the UK because electricity costs too much here for crypto mining to really be profitable, so that is not really a consideration for the UK.

Financial regulation is absolutely a consideration, and particularly protection for consumers. There are a lot of well-meaning people, but there are a lot of predators out there, so, absolutely, protect the public.

On the enterprise blockchain thing, the words to keep repeating to yourself are, "magic does not happen." If someone comes and tells you that a technology will magically increase your organisational efficiency and make bureaucracy magically easy, you know better than that. Magic does not happen.

Dr Robinson: I agree. We need to have a clear and comprehensive regulatory framework for all aspects of crypto activities—AML, trading, consumer protection. We currently do not have that. We have all the ingredients to be a leader in this industry, but we have squandered that to a certain extent so far, and businesses are leaving the UK for other jurisdictions. We need to take the lead on regulation rather than waiting for international consensus to develop and then following that.

Q75   **Chair:** Perhaps Dr Robinson will permit me a personal question. We are very interested in this Committee on careers in science and technology. You are an Oxford doctorate in physics, I think, and you went on to co-found your company. What was your entry into this world? Was it through your degree? Tell us about your journey.

Dr Robinson: Like a lot of people with a physics background in the UK, I ended up in finance. I had the technological background combined with experience of working for a regulated financial institution. When I saw crypto, I saw the need and the opportunity to help it thrive in a regulated environment, and that was the origin of Elliptic.

Q76   **Chair:** I see. You did your physics DPhil, and then you went into the City, did you?

Dr Robinson: Yes.

Chair: And from that into blockchain.

Thank you both very much indeed for your evidence today. It has been very enlightening.

Examination of witnesses

Witnesses: Professor Naughton and Craig O'Kane.

Q77   **Chair:** We are now going to turn to our final pair of witnesses, whom I am pleased to introduce. We have joining us virtually from Brisbane—and I see him on the line—Craig O'Kane, the chief operating officer for Everledger, a company that provides services using blockchain.

Joining us in the room is Professor John Naughton. Professor Naughton is a senior research fellow at the University of Cambridge and has written extensively on technology and its role in society, and on the history of the internet. Thank you very much, both of you, for joining.

It is obvious that Mr O'Kane has commercial interests. Since you are here with your academic hat on, Professor Naughton, just for the record, do you have any commercial investments or interests in this space?

Professor Naughton: Absolutely none.

Q78   **Chair:** Very good. Thank you very much indeed. Perhaps I could start with an initial question to Mr O'Kane. Perhaps you could introduce Everledger and outline how it uses blockchain and distributed ledger technology, which has been the subject of our inquiry this morning.

Craig O'Kane: Thank you very much, Chair. Good evening from the time zone where I am based.

Everledger is known as a blockchain company and has been in operation since 2015. It has grown since that time to around 70 staff globally in about five different countries. We use a different type of blockchain from what has been discussed so far, which is private permission ledger on

Hyperledger. It is not crypto. It is not a bitcoin. It is not in the public ledger environment. We are not involved in DeFi. We provide trust, transparency and traceability on a platform of provenance.

We started with diamonds—there are some reasons why we started with diamonds—linking specific objects to the blockchain. We have moved into gemstones, pearls, high fashion—apparel—wine and spirits, and much more recently into the wool industry and the wool supply chain in Australia, critical minerals in Australia, and battery passport technology.

Q79   **Chair:** Thank you. You may have heard in the last session that we heard, especially from Mr Gerard, some scepticism that the distributed ledger technology has added anything much to the underlying questions about the assets in the supply chain. Would you answer that and say how what you do does things in a different and better way than perhaps more conventional means of certifying diamonds?

Craig O'Kane: Our blockchain technology as an enterprise solution using Hyperledger is still evolving. On a Hyperledger Fabric framework that we are operating on, we are working with our partners, including those involved in its development. It is an open-source type of technology initially built by Linux, IBM, Intel and SAP. Now, there are many other contributors to enterprise solution technology.

We are really careful and particular about the types of companies and the types of nodes that are on our platform.

As an example, if we are talking about the critical mineral space, we have just done a big piece of work for the Australian Government in critical minerals. That solution looked at bringing together miners, processors, standards bodies, OEMs and the Government into an environment where they can surface information such as claims related to those objects such as critical minerals, including things like origin.

Q80   **Chair:** What is the problem to which you have the solution? What prevents that from being done in conventional means?

Craig O'Kane: In that particular piece of work, we conducted around 300 separate interviews in looking at the problem. The problem is that there is no single space or place for anyone in that ecosystem—in that value chain or that supply chain—to be able to show, tell or sell their goods' story with the emphasis on "good": a way to differentiate these supply chains in a way that is understood by multiple different parties and actors in that supply chain.

At the moment, claims might be substantiated at the end of an annual report or a sustainability report, and those reports are only as good as, let us say, what a mining company surfaces or provides to financiers or to the Government. The blockchain enables those parties that are on the nodes of that enterprise solution to attest, validate and verify the claims that that company is purporting and putting out there. It is the additional method of verification in an enclosed environment.

Q81   **Chair:** If third parties had doubts about claims that were being made in an annual report, surely there are mechanisms that are available. The supervisory bodies in every country for listings—

Craig O'Kane: Absolutely.

Chair: —would be very concerned to hear that claims were made in an annual report that did not stand up to scrutiny. Why does that need a distributed ledger technology to operate it?

Craig O'Kane: The way in which a company might have additional scrutiny placed on those claims that it is purporting might result in a manufacturer downstream in the value chain like Apple or Tesla then validating for themselves the claims that a mining company or a processor is making. That might result in five to 10 additional reports that are written and people travelling from the manufacturers themselves to a site in order to validate for themselves what they need to know as opposed to just relying on facts that have been presented at that time. It is a reduction in the cost and the time by using the blockchain to validate and verify substantiated claims as opposed to doing increased numbers of checks.

Q82   **Chair:** How does that rely on the blockchain? Is that not just the equivalent of a review site like Tripadvisor or Trustpilot on to which people with different experiences can upload, in a way that is accessible to others, their experiences of the claims that someone providing a service has given? That does not require blockchain; it requires a website or a platform.

Craig O'Kane: Absolutely. We are not trying to remove reviews or prevent other assessment bodies or different types of standards agencies from doing their jobs. They are perfectly capable of doing that. It is a complementary network in order to provide substantiated, immutable claims for the right people to see within a noded network.

The other thing is that the system is agnostic to the types of standards that we would like to ingest. Is data that is being collected and ingested by the distributed ledger happy for as many different types of standards and claims to be presented to it, so that people can make their own choices about whether those ESG claims are the ones that they want to see?

Q83   **Tracey Crouch:** Following on from the Chair's last question and your answer to it, how important is the accuracy and quality of data to ensuring that you and other firms can make the most of the blockchain technology?

Craig O'Kane: It is important. It is a network based on trust and transparency. For the way in which a mining company, a processor, a standards body, an OEM and a Government Department is part of a network, the data is really important. In the normal world, we might find that a mining company needs to provide information to the Government,

such as information on CO_2 emissions, information on its water usage and information on a whole variety of things.

The information that they are demanding already is a matter of fact. We need to be able to ensure that the data being provided is accurate. The blockchain is allowing for greater efficiencies in the fact that the mining company might only provide that once to the platform so that many other parties on the blockchain can also inspect that data.

Q84 **Tracey Crouch:** Thank you. Professor Naughton, you have previously written that the blockchain idea evokes utopian hopes. Could you briefly outline why that is the case?

Professor Naughton: Thank you. You have to put this in a wider context. One of the things one needs to bear in mind is that this technology emerges from a very small and very specialised part of the world, which is largely dominated by, I am sorry to say, people like me. I am an engineer. There is a prevailing mindset that is really common in Silicon Valley and its associated areas, which is that for every problem—every social problem and every other kind of problem—there is a technological solution. It is called solutionism as a mindset and it is very prevalent. One sees it everywhere.

One way of looking at this current wave of innovation, concern and hysterical enthusiasm is that we live in an untrustworthy world and in a world where our banking systems were imperilled by the loosely regulated and reckless behaviour of banks, which we eventually had to bail out in 2008. The institutions that are supposed to oversee our world are in many cases untrustworthy, and maybe there is a way of solving this problem by using technology.

You can see it as a utopian vision—that it is possible to solve this problem by just using technology. It is utopian in the sense of all utopian dreams, which is that it is actually unrealisable, but that does not stop it being very seductive.

I describe myself as a recovering utopian because I was a very early enthusiast for the internet, and some of my friends and contemporaries built it, and we thought at the very beginning that we had created something that was truly transformative, liberating, democratising and empowering for people. All of that is true, but it has not worked out like that exactly.

The same applies to this particular obsession. That does not mean that many of the people are not honourable, enthusiastic and clever. All of that is true. If you look at this in the wider perspective, you see the same thing—a technocratic belief that technology has a solution to a problem that has always been widespread in our societies and we always have to solve.

Q85 **Rebecca Long Bailey:** Professor Naughton, you mentioned the banking

crash. There was a lot of discussion in the previous panels about trust and transparency and how blockchain systems can build up trust and transparency, particularly within the financial sector. I know that you have identified two main challenges associated with the technology—technical and governance. Could you elaborate on that and the risks that you see in the future?

Professor Naughton: First of all, to go back to the trust aspect of your question, in a system of financial exchange there has to be a way of trusting between the different parties with whom you are engaged; and, secondly, there has to be some way of enforcing contracts and of punishing non-compliance and all that kind of stuff. We have methods for doing that in general, which we implement imperfectly at times. The idea that somehow a blockchain is a way of providing trust that can always be relied upon is a myth.

You talked in the previous session about the way in which adding blocks to a particular kind of blockchain requires a lot of computing. It does, but the point is that there is still authority in the system because a block has to be verified by consensus as being valid.

Where does the authority reside? In this case, it resides in the code of the blockchain. Who writes the code, and are there circumstances in which the consensus mechanism can be hijacked? The answer is "yes". It is unlikely, but it is "yes". If it is a proof of work validation, it turns out that the participants in the blockchain who have most resources have more of a vote in how things are verified, and so on.

There is no escape from the need for authority. What is happening is an attempt to displace that sort of authority from democratically accountable institutions like regulators, which are set up by Governments. That is the core bit of the problem. There is no question that the technology is ingenious, but it is not a solution to the trust problem. It is also not terribly transparent. Just thinking about cryptographic technology as being transparent to the average human being is a bit rich.

As the previous session indicated, a lot of people in this business, many of them unscrupulous, are trading on the fact that somehow because it is impenetrable it is somehow profound. That is not true.

One of the difficulties we all have with this is that we are not seeing it in a wider context. There have been these kinds of technological improvements many times. They all follow the pattern that is described in the famous hype cycle devised by Gartner, where something starts, it is very exciting, you get a huge surge of irrational expectations for it, which eventually peak, then it goes into a decline—into what Gartner calls a trough of disillusionment—and it starts to slowly rise as people discover that some of this is useful and some of it would be of social benefit or commercial benefit and we can get to it.

That is the cycle we are going through with this stuff now, and we will eventually get to the point where there are some things that we recognise from it that are useful and valid, but, in general, we are not there yet.

If you want a model for it, there was a time when relational databases were considered to be very exotic and very new and had all the excitement rather like blockchain, and now it is impossible to find an organisation that does not routinely use relational databases. My hunch is that that is what will happen with blockchain. It will eventually become very boring and very common in certain kinds of applications, and it will be avoided for others.

Q86 **Rebecca Long Bailey:** Mr O'Kane, we have just heard about some of the main challenges associated with the technology today. Do you think that they are being properly addressed, particularly at an international level, where it is very difficult to assess different Government approaches?

Craig O'Kane: It is an emerging technology and needs additional scrutiny and understanding. There are many different work groups that exist already looking at its potential, including the World Economic Forum, the OECD and the European Commission. There is a lot of work already occurring in this space.

Q87 **Rebecca Long Bailey:** Sorry, those are our bells. All we have are bells going off in Parliament constantly throughout the day letting us know that we need to be doing certain things.

You mentioned the issue of trust and transparency, and that is definitely a theme throughout the panels that we have been listening to today. In keeping with that theme, with your current business model, you mentioned being able to prove throughout the blockchain details regarding particular sources.

For example, for a diamond mining company, you would be able to source all the way back through your blockchain the mine that that particular diamond came from. How would you do that, and how would that be policed? Who would be the enforcer?

Craig O'Kane: The blockchain itself is the enforcer. How we do it is a very good question. Given that it is evolving, obviously, there are additional steps that we continuously make in order to surface the truth around objects. We can attach RFIDs and NFCs to some objects. It is the same chip you have in your credit card and Oyster card. There are ways that you can link the physical to the digital in order to be able to substantiate that that object is what it says it is. That could be in a garment, for example.

The reason you do something like that is not only to have an interactive and great experience as a customer with the company being able to communicate with you and send you messages rather than just emails, but for circularity. If there is a better use for that garment in the future,

or if you then go to sell that particular object to somebody else, the chain of custody is going with it because there is a way that the physical object is linked to a digital object.

In the case of diamonds, we already know a lot about graded diamonds. We already know a lot about mining practices based on things like the Kimberley Process and on the evolution of that very dark murky sector over a period of time that continues to try to surface additional transparency just because of the very nature of what it is.

You have mechanisms. As a rock is taken out of the ground, that is an event. You can capture the date and the timestamp of that event. When that object is then sent to a cutter and a polisher and there is a transportation process and there is a chain of custody, that is another event. Again, that information can be taken and placed on the ledger.

At the point where it is then polished and cut, the grading individual and the grading house will have their say on that object. The four Cs of that diamond will be established. A laser inscription will be placed inside that diamond. In fact, most diamonds have a laser inscription to link the physical object to the digital platform. There are different ways you can do that.

Some companies will have used things like a QR code. Other companies might use an additive. There are tracers. There are isotopes when you are talking about particular critical minerals from particular locations in the world. There are a variety of ways that you can link physical objects to digital twins.

Q88   **Rebecca Long Bailey:** Is it voluntary? The company that wants to be part of the blockchain would voluntarily give you that information. When they took the diamond out of the ground, they would issue you with whatever copy of whatever certificate they have allegedly to prove that that happened, and that would simply be attached to the blockchain. Is that right?

Craig O'Kane: There are two ways of answering that. We have our blockchain platform available for retailers that might want to be able to surface and substantiate those claims. It is by choice. A company such as diamonds.co.nz or Brilliant Earth might elect to sell blockchain-enabled diamonds. Their customers might say, "I would like to know where that diamond came from and that modern slavery or child labour was not used in its extraction process. I want to know that it is not Russian. I want to know that it is from a source that I am proud of and I am willing to buy from." Some companies will elect to do that, and they might try to use our blockchain technology to surface those claims.

In other examples, in an enterprise environment, it might not be voluntary, and you might have an enterprise solution built for a particular company that is requiring certain types of information before they receive

an object based on the chain-of-custody events that have taken place before it. There are different types of blockchain for different use cases.

Rebecca Long Bailey: Thank you, that is really helpful.

Q89 **Chris Clarkson:** Craig, notwithstanding your own work, are there any countries or initiatives that you would highlight as having been particularly innovative in the use of this technology? What lessons do you think the UK could learn off the back of those?

Craig O'Kane: We have been very lucky to work in a couple of jurisdictions internationally. In the Department of Energy in the United States and in Australia, where I am currently based, there have been experimentation opportunities with pilots, which some of the other witnesses spoke about before.

We are very interested in what is occurring in the space of greenhouse gas emissions and scope 3 reporting. For critical minerals that are being mined in Australia that might be utilised in Europe by a particular OEM manufacturing a product that requires critical minerals like lithium, cobalt, vanadium and nickel, there are ways in which you can provide that greater transparency that it is from a mining site in Australia, it has been through a transformation process, and now it has ended up at Jaguar Land Rover or JCB or whoever requires these critical minerals.

In the US, the work we did was with battery passport technology. At the other end of the use case in minerals, you might have batteries that are used in a vehicle for eight years and they deplete. What is the best way to ensure you are disposing, repurposing or recycling that battery that contains those particular minerals in the right way? There might be a trust issue if you were to take that battery out and just put it in the tip.

There might be an opportunity for that particular battery that contains these quantities of minerals for another use. Maybe it is in a home battery-powered solution in a domestic sense. Because these minerals are finite, we see a greater need and a greater understanding that we just cannot keep mining. We need to be able to link certain physical objects such as batteries in a way to strive for circularity. They are a couple of examples that we have been involved with in the US and in Australia.

Q90 **Chris Clarkson:** Thanks, Craig. Those are very interesting examples as an assurance piece as much as anything.

Can I put this question to both witnesses? If you could suggest one priority for the UK Government as we think about this area, what would it be?

Professor Naughton: Rather like one of the previous panellists said, in relation to cryptocurrencies, NFTs and virtual products like that, consumer protection is the prime thing. If that is not attended to, we will continue to see an increasing spate of exploitation of people. A lot of

people are going to lose a lot of money if Governments do not act. That is the prime thing.

On the other front, the difficulty with blockchain technology, which is at the core of all of this, is that it is potentially a very useful technology. The kind of use case that Mr O'Kane set out is a really good one. There are all kinds of other ones such as food security.

In China, where they have, it seems, a serious problem with food security, there was a very interesting experiment where a particular entrepreneur who ran a chicken farm wanted to be able to sell his chickens as free-range. He put an electronic tag that counts the number of steps that a chicken takes on the leg of every chicken. That is encoded on a blockchain. When the consumer buys a chicken, they know that this chicken has been running around quite a lot. That is a frivolous example, but the point is that there are really important and compelling use cases for this technology. There are also compelling cases for not using it. For example, it should not ever be used for holding personal data.

Chris Clarkson: I would agree with that.

Professor Naughton: Countries like the UK need to have some kind of pre-emptive unit that thinks ahead rather than having to respond when stuff has happened. I saw some encouraging signs with the Competition and Markets Authority in that respect. Countries need a different kind of approach to regulation. Sometimes they have to look ahead to see what might be coming down the track and what might cause problems. It is more like a laboratory view of these things. My hunch is that because regulators are generally staffed by lawyers they are not that good at that. We need a different sort of attitude towards this.

Chair: I am sorry to press you, but we need to make sure that we get through our remaining questions.

Q91   **Chris Clarkson:** On behalf of this lawyer, thank you. Craig, is there anything you would like to add?

Craig O'Kane: I am not in the crypto space, Bitcoin or Ethereum, so I will take the other witnesses' comments on that. For the UK, it would be really interesting to look at two things. One is the growth and the rise of regulatory requirements, particularly in ESG, greenhouse gas emissions and CO_2, and the quantity of regulation that is being demanded, not just through things like mandating everybody in the UK to buy electric vehicles in the future, but the carbon border adjustment mechanism that the European Union is talking about, the German Government's Supply Chain Due Diligence Act, and the US State Department's controls on CO_2 imports. I really do think that is something that the UK should be across, at least.

The other thing is purely geopolitical risk in supply chains—looking at which countries around the world the UK would like to do more business

with and which economies it might not want to do business with. I feel as though we are definitely in a space where we can see tensions in this sector around things like the minerals used in batteries.

Q92   **Aaron Bell:** I have a couple of brief questions to Mr O'Kane. You are obviously not in the financial space. Are you worried at all that the current crypto crash and the coverage of that damages the standing of the technology as a whole?

Craig O'Kane: Absolutely. There is no question but that blockchain is bundled into one pot and it gets stirred. The original intent in the use case for blockchain was not something like crypto and how that has now taken over and everyone talks about blockchain and crypto in a mass marketplace. It gets all mixed in together, and I feel as though the current hype and the collapse of certain cryptos paint a poorer picture for this industry.

Q93   **Aaron Bell:** Thank you. Turning to you, Professor Naughton, I was struck by your comparison with the internet. There might not be a central authority, but there are rules, and the question is who sets the rules, and that is, ultimately, a political question. How should politicians like me or the Chair be addressing these issues?

Professor Naughton: They should not be intimidated by the technology per se. The fundamental issues in all of this—for example, the question of trust, authority and regulation—may be different in detail, but the principles are the same. One of the difficulties democratic states have had in the last two decades is that they have been too intimidated by the rapid growth of the technology. We have reached a point where a narrative has taken hold, and the narrative says that technology drives history and society's job is to sweep up after it like those Indians who used to walk behind the maharaja's elephant.

The real question we should have as a democracy is what things we will allow and what things we will not allow. We already do that in some areas. I think we will get to the point where we have to consider that in relation to this technology, not just blockchain and not just cryptocurrencies, but the technology as a whole. What are the things we will allow? We do not allow just anybody to make medicine.

Q94   **Aaron Bell:** The Government have been strikingly quite positive over the last six or seven years. There was a report called "Distributed Ledger Technology: beyond block chain" in September 2016. Only a few months ago, the Government announced plans "to make the UK a global crypto asset technology hub", and yet Select Committees such as this one and the Treasury Committee have been notably more cautious, and we have heard that today. Do you think the Government are being a little naive, or are they simply keeping an open mind?

Professor Naughton: My view is that the Government in this space have been naive and boisterous for two decades. There was a time when every functioning leader of the Government wanted to get an invitation to

Google. Before that, more old-fashioned Governments wanted an invitation to Microsoft.

That period is over because it has dawned on the world that this technology is both powerful and dangerous. At the moment, there is too much sloganeering about making the UK the centre of whatever it is at the passing moment. This is complicated stuff. It is really important, and sloganeering does not do it.

Aaron Bell: Thank you very much.

Chair: Thank you very much indeed, Professor Naughton, and, in Brisbane, Mr O'Kane. We are very grateful for your evidence, as we are to all of our witnesses in today's short, focused but very enlightening session on blockchain. We will reflect on the evidence that we have heard and make some recommendations to policymakers accordingly.