Back to article page

London Review of Books

When Bitcoin Grows Up

John Lanchester

It's impossible to discuss new developments in money without thinking for a moment about what money is. The best place to start thinking about that is with money itself. Consider the UK's most common paper money, the English five or ten or twenty quid note. On one side we have a famous dead person: Elizabeth Fry or Charles Darwin or Adam Smith, depending on whether it's a five or ten or twenty. On the other we have a picture of the queen, and just above that the words 'I promise to pay the bearer on demand the sum of', and then the value of the note, and the signature of the cashier of the Bank of England.

It's worth thinking about that promise to 'pay the bearer on demand the sum of ten pounds'. When we parse it, it's not clear what it means. Ten pounds of what? We've already got ten pounds. That's exactly what we're holding in our hand. It doesn't mean, pay the bearer on demand ten pounds' worth of gold: the link between currency and gold was ended in 1971, and anyway, Gordon Brown sold off the Bank of England's gold reserves in the 1990s.

The fact is, there's no answer to the question, ten pounds of what? The ten pound note is worth what it claims it is because the state, in the form of the Bank of England, says so, and we choose to believe it. This is what students of currency call 'fiat' money, money whose value has been willed into being by the state. The value of fiat money is an act of faith. There are quirks to this. In the case of the pound coin, if we ask how much it's worth, the answer is obvious: a pound is worth a pound. It shouldn't be, though. According to the Royal Mint, which actually makes the stuff, 3 per cent of all pound coins in circulation are fake. Allowing for that, we should discount the price of our pound coin, and mathematically assign it a value of 97p.

In real life, there's no need to do that, because the overwhelming probability is that you won't have any difficulty spending your fake pound for its full nominal value. (That's unless you're caught out by a coin slot which rejects your money. Most people attribute the annoying frequency with which this happens to a problem with coin slots; mostly, though, it's a problem with the currency. The other time you'll have trouble with your fake coin is when you get one of the mutant squishy ones which look like partially chewed fruit pastilles and are so badly forged they verge on the endearing.) They're worth what they claim because we choose to believe in them. Your mathematically determined 97p of coin is worth a quid because we believe it's worth a quid. We trust it. That's the first main point about money. Its value rests on our belief in its value, underwritten by the authority of the state.

For the second main point about the nature of money, we need to travel to the Pacific Ocean. In Micronesia, about 1800 miles north of the eastern corner of Australia, there's a group of islands called Yap. It has a population of 11,000 and is largely unvisited except by divers, but it's a very popular place with economists talking about the nature of money, starting with a fascinating paper by Milton Friedman, 'The Island of Stone Money', published in 1991. There's a particularly good retelling of the story by Felix Martin in his 2013 book *Money: The Unauthorised Biography*.

Yap has no metal. There's nothing to make into coins. What the Yapese do instead is sail 250 miles to an island called Palau, where there's a particular kind of limestone not available on their home island. They quarry the limestone, and then shape it into circular wheel-like forms with a hole in the middle, called *fei*. Some of these fei stones are absolutely huge, fully 12 feet across. Then they sail the fei back to Yap, where they're used as money.

The great advantage of the fei being made from this particular stone is that they're impossible to counterfeit, because there's none of the limestone on Yap. The fei are rare and difficult to get by definition, so they hold their value well. You can't fake a fei. Just as you have to work to get money in a developed economy – so the money constitutes a record of labour – the fei are an unfakeable record of the labour that went into their creation. In addition, the big ones have the advantage that they're impossible to steal. By the same token, though, they're impossible to move, so what happens is that if you want to spend some of the money, you just agree that somebody else now owns the coin. A coin sitting outside somebody's house can be transferred backwards and forwards as part of a series of transactions, and all that actually happens is that people change their minds about who now owns it. Everyone agrees that the money has been transferred. The real money isn't the fei, but the idea of who owns the fei. The register of ownership, held in the community memory, is the money.

It has sometimes happened to the Yapese that their boats are hit by stormy weather on the way back from Palau, and to save their own lives, the men have to chuck the big stones overboard. But when they get back to Palau they report what happened, and everyone accepts it, and the ownership of the stone is assigned to whoever quarried it, and the stone can still be used as a valid form of money because ownership can be exchanged even though the actual stone is five miles down at the bottom of the Pacific.

That example seems bizarre, because the details are so vivid and exotic, but our money functions in the same way. The register is the money. This is the second main point about the nature of money. We think of money as being the stuff in our wallets and purses; but most money isn't that. It's not notes and coins. In 2006, for instance, the total amount of money in the world in terms of value was $473 trillion. That's a number so big it's very difficult to get your head round: about £45,000 per head for all seven billion people on the planet. Of that $473 trillion, less than a tenth, about $46 trillion, was cash in the form of banknotes and coins. More than 90 per cent of money isn't money in a physical sense. That number is even bigger in the UK, where only about 4 per cent of money is in the form of cash. What it is instead is entries on a ledger. It's numbers on your bank balance, the electronic records of debits and credits that are created every time we spend money.

When we say we spend money, what we're mainly doing is making entries on registers. Your work results in a weekly or monthly credit from your employer's account to your account, maybe with another transfer of PAYE tax to the government, also your pension contribution if you make one, any forms of insurance, then a chunk automatically going off to your landlord or mortgage provider – all heading to different parts of the financial system, all of them nothing other than movement between and among all these various ledgers and registers. This is what almost all of what we call money mainly is: numbers moving on registers. It's the same system they have on Yap.

The third point is that money as it has evolved has a crucial relationship with technology. There are a number of technologies that are inexorably interwoven with the working of money. The first of them, probably the most important piece of technology in human history, is writing. This begins in ancient Sumer, about three thousand BC, with records of trade and inventory gradually evolving into other kinds of recorded script. The next big invention arrives in Renaissance Italy, with the popularisation of the balance sheet, and with that, of banks that become places where all the different transactions in a society, all the various credits and debits, are gathered together in a single register. The bank becomes the intermediary between creditors who have spare money to lend and borrowers who have reasons for needing it. Instead of a near infinite multiplicity of transactions between individuals, swapping credits and debits backwards and forwards as we exchange goods and services and IOUs, promises and debts and obligations, one to one, all the various transactions in all the various markets of a complex social environment are now held on the books of one institution: the bank. The society has one register, and that register is run by the bank. Arguably the first really successful example, the first to deploy the new technology of record-keeping effectively, was the Medici bank in Florence.

The final piece to this is the invention of the central bank, with the foundation of the Bank of England in 1694. In return for lending the sovereign a great deal of gold, in the first instance to build a navy to fight the French, the Bank of England acquired the right to print paper money. That paper money could then be used by ordinary people to pay their taxes. It's at this point that banks, money and the modern state become fused together. The money system and the banks and the state are all in effect aspects of one another: a triple-headed monster, like Cerberus.

Short historical digression: it took a while for this system to spread everywhere, especially in the United States, where arguments about the link between the banks and the state and the money system have been a recurring theme. In *How Would You Like to Pay*, a lucid short book on new money technologies, Bill Maurer points out that as recently as the

1860s the United States had eight thousand private currencies in circulation, issued by 'banks, railroad companies, retail stores and other entities'.[1] There is an interesting discussion of US money in Edward Castronova's overview *Wildcat Currency*: he explains that states didn't have the right to issue currency themselves, but they did have the right to regulate the issuance of money on their territory.[2] This was a system prone to unintended consequences. Several states

> permitted banks to issue money only in large denominations. This was done to force banks to retain adequate gold reserves. The theory was that holders of large denomination bills were more likely to return to the bank and exchange those bills for gold. As a result banks would have to keep more gold on hand. A bank with more reserves is less likely to fail.

That was the theory. The practice: many of the new denomination notes were too big to use. As a result, there was a huge proliferation in private money, issued by everyone from farmers and merchants to hotels and restaurants and bars. An ordinary person's wallet might contain a dozen different currencies, all worth different amounts in different places, since a bar's money might trade at full value in the bar itself, but would be worth significantly less the second you stepped out the door – and less still as you moved further and further away. The government response, in 1851, was to create a three cent coin, the trime. It was only after 1864, when Congress banned the issuance of metal coinage for money, that private money began to be driven out of the economy.

In time, even the US joined the system of state-backed money dispensed through a central bank. This is the system we still have everywhere in the developed world today. The reason a lot of people are excited about bitcoin and its associated technologies is that for the first time there is a genuine possibility of real change in this area. Money has evolved in jumps, from the invention of writing to the invention of the balance sheet and the bank to the creation of the central bank, with all of these changes being variations on the theme of money as a register of credits and debits. And we're now at a point when another jump is possible.

The simplest and biggest possibilities concern connectivity. We are more connected in more ways to more people than we ever have been at any point in human history. This is changing everything, and it would be deeply strange if it didn't change money too. There are many ways in which the impact could happen. For instance, a huge part of the money system is about intermediaries. It goes back to the Medici, to that central register where the debits and credits are all gathered together in one place. The bank is the intermediary between creditors and debtors. Obvious question: do we still need that intermediary? I have money I'm not using, you need more credit than you have, to buy a house or start a business or buy a car or whatever. I lend you the money, and you pay me back. Easy-peasy. We have historically needed a bank to mediate that transaction, and to take a generous cut in the process. It's not at all obvious that we need it any more. We can find each other without the bank in the middle; thanks to the internet, we can locate each other without intermediaries. It seems very obvious to me that this area, that of P2P or peer-to-peer lending, is going to grow and grow. Why lend money to your bank for fuck-all interest when you can go to Zopa, the UK's leading P2P site, and lend it directly to someone who needs it, for a return of 5 per cent? The answer at the moment is probably that the banks are old and have some deposit protection, whereas online lending is new and doesn't. But that answer is not writ in stone, and one lesson of the internet is that when customers' behaviour changes, it can change fast. A lot of money is at stake here. The cut being taken when A sends money to B amounts to $1.7 trillion – that's right, trillion – every year.

Connectivity has implications for other kinds of transfer too. Money is a way of transferring credit. New forms of doing that directly are now possible. The great trailblazers for this are in the developing world, especially Kenya, which has adopted a form of direct transfer called M-Pesa. This involves the transfer of credits not from bank account to bank account, but from one mobile phone to another. M-Pesa was introduced in 2007, and took off in popularity when violent chaos following the elections at the end of that year brought the regular banking system to a halt. That's an example of the way chaos and uncertainty around traditional banking creates appetite for new services – not so different from the United States, where the Civil War made private money finally unviable. A few years after its adoption, M-Pesa is the conduit for half of Kenya's GDP. Credit goes from phone to phone, and that credit is a new form of money, making the kinds of facility you get from a bank account available to all sorts of people who don't have one. Once you have a record of successful payments on your phone, merchants and institutions will take that as a sign you can be extended other forms of credit, and you can start to move from the informal economy where the poor are trapped – where there are no records of their credit, no records of what they own – to the wider economy. That's huge.

The world's population is seven billion. Two and a half billion adults don't have a bank account. Paul Vigna and Michael Casey's excellent book *Cryptocurrency* explains what that means:[3]

> Somewhere in the order of five billion people belong to the households that are cut off from a financial system that the rest of us take for granted. They can't start savings accounts. They don't have checking accounts. They can't get credit cards. They live in places where banks don't want to go, and because of this, they remain effectively walled off from the global economy.

But there are at least seven billion mobile phone subscriptions in the world (four and a half billion people have access to a flush toilet). So more than twice as many people have a mobile phone as have access to a bank account. If your phone can give you access to the things you would need from a bank, well, you've just disinvented the need for banks, and fundamentally changed the operation of the money system, across whole swathes of the developing and emerging world.

The reason phones can do this is because they embody a remarkably high level of trust. You can trust that the phone is the property of the person who owns it, because the combination of sim card technology and pin numbers is very strong. Behind the user-friendly façade of chip and pin are cryptographic techniques of industrial strength. Indeed, the pin number technology used in cashpoint machines initially evolved as a question and response protocol to confirm nuclear weapon access codes. You can trust that this person who owns the phone is who they say they are: that basic act of trust is fundamental to the operation of all money systems.

What's making this possible is cryptography. Cryptography is also central to one of the most interesting developments in the world of money, and that is bitcoin. I'm not sure whether bitcoin is likely to be the most consequential of all these developments: peer-to-peer lending, and non-bank payment systems of the M-Pesa type, seem to me at least as likely to change lives, especially the lives of the poor. But there's no denying that bitcoin is the best story.

*

Bitcoin is a new form of electronic money, launched in a paper published on 31 October 2008 by a pseudonymous person or persons calling himself, herself or themselves Satoshi Nakamoto. Note the date: this was shortly after the collapse of Lehman Brothers on 15 September, and the near death of the global financial system. Just as the Civil War was the prompt for the United States to end private money, and the crisis of Kenyan democracy led to the explosive growth of M-Pesa, the global financial crisis seems to have been a crucial spur, if not to the development of bitcoin, then certainly to the timing of its launch.

Bitcoin's central and most exciting piece of technology is something called the blockchain. This is a register of all the bitcoin transactions that have ever happened. Every time something is bought or sold using bitcoin – remember, that means every time something moves from one place in the register to somewhere else – the new transaction is added to the blockchain and authenticated by a network of computers. The techniques are cryptographic. It's impossible to fake a new addition to the chain, but it's relatively easy (by relatively easy, I mean relatively easy for a huge assembled array of computing power) to verify a legitimate transaction. So: impossible to fake but simple to verify. The entities transferring the money are anonymous, and at the same time completely transparent: anyone can see the bitcoin addresses involved, but nobody necessarily knows to whom they belong.

This combination of features has extraordinary power. It means that you can trust the blockchain, while knowing nothing about anyone else attached to it. Bitcoin is in effect a register like the one kept in people's memory on Yap, but it's a register that anyone can see and to which everyone assents. For the first time in human history, we have a register that does not need to be underwritten by some form of authority or state power, other than itself – and, as I've argued, that register isn't some glossy add-on to the nature of money, it actually is how money works. A decentralised, anonymous, self-verifying and completely reliable register of this sort is the biggest potential change to the money system since the Medici. It's banking without banks, and money without money. The next several paragraphs give a short technical explanation of how bitcoin works; if you aren't interested, see you at the dropped letter.

The profoundest mystery about the physical universe is that it is so intertwined with mathematics. Gravity is inversely proportional to the square of the distance between two objects. Why? Why does pi, essential in calculating the circumference of a circle, also prove essential to calculating the area of a circle: why is it an exact value, not just a rough guide or rule of thumb? Why does it also turn up in so many other places in mathematics? Why, for instance, is the probability that two random numbers have no common factor equal to $6/\pi^2$?

We don't know why maths reaches so deeply into the texture of physical reality. One of the hardest things to understand about cryptography is that it rests on something that is inexplicable, and that is *it works*. As Julian Assange has said,

> it just happens to be a fact about reality, such as that you can build atomic bombs, that there are math problems that you can create that even the strongest state cannot break … there is a property of the universe that is on the side of privacy, because some encryption algorithms are impossible for any government to break, ever.

The effectiveness of cryptography in essence rests on a single truth about mathematics: that it is impossible to factorise big numbers. For any number, there is no way of working out if a smaller number divides into it, short of actually doing the calculation. This might sound like a small point, but it means that when you have very long numbers – numbers that are hundreds or thousands of digits long – there is no way of breaking them down into factors other than by trying every smaller number and seeing if it fits. With very very big numbers, that process is, in practice, impossibly time-consuming. This makes very long numbers, and the prime numbers which are their factors, into miraculously effective cryptographical entities; the basis for all contemporary codes. This is in turn a hard fact for civilians to swallow, notwithstanding that it underlies more or less everything we do, in business terms, on the internet. (Note that having secure codes is not the same as having secure computers. Breaking into people's computers is a completely different story from breaking their codes – and once you've broken in, it often doesn't matter what the host is doing cryptographically.) To grasp bitcoin – or to believe in bitcoin – you do have to take this power on trust.

*

There are three main crypto-mathematical techniques at work in bitcoin. The first is the matching of a public address – that's the bitcoin address of any given user – with a private key which provides access to that address. Although the cryptography involved in this process is fearsome, drawing on those aforementioned properties of prime numbers, it is so widely used – every time you use a credit card, every time you use a pin number – that we'll just take it for granted here. When you spend some bitcoin, all you're really doing is changing an entry on a digital register from address A to address B: at that point, your transaction is broadcast to the network, where it takes its turn with other transactions waiting to be compiled into a ten-minute chunk of transactions, known as a 'block'.

This is where the miners come in. ('Mining' is a bad metaphor for what these computers do: it's more like clerking or verification. But mining is what it's called.) Miners take this ten-minute block of transactions, each of which combines the two addresses of the parties to the transaction, the quantity of bitcoin moved and a time stamp, and run them through a 'hash function'. These are cryptographical algorithms for encoding information: the one bitcoin uses is called SHA-256. The hash function takes a stream of information of any length and turns it into a unique set of letters and numbers, of a fixed length. Here is 'The cat sat on the mat' run through SHA-256: 500532af74c472e39c7d685fddb727c3bf461ce41118f29f856bafe4024fc303. And here for purposes of comparison is 'The cit sat on the mat': a8727c0891cec28e10c03 aa09c759d92fd628e131435b502c04e60d 09ce4ef76.

As we can see, the output is sensitive to any change in the input: alter so much as a single letter and the entire hash changes. Note that however long and complicated the input, the output is always 64 characters long. Just to make the point, here is SHA-256 hash of the entire text of *Ulysses*: 6ff1c1a80b68b5414423a7e2e061d5f2f c09f7c4e86c4987e573bebc4e4991dd. Put all this together, and you have a system which makes it very easy to check whether a given text has been hashed correctly: you just run it through the algorithm. At the same time it is impossible to guess the input from the output. There are just too many possibilities: it is mathematically impossible to land on the correct one. Anyone can check the hash function of *Ulysses* online in about ten seconds. Every computer in the world linked together could not reverse the encryption, and work out that the input behind the hash is Joyce's novel. This is just a glimpse of the magic power of encryption.

Miners take the transactions in the block, hash them, and add them to the hash of all the transactions that have ever happened in bitcoin. That's right: the blockchain is a register of every transaction, however small, which has ever happened in the currency. The miners then run the hash through a calculation, set up by Satoshi, which makes them come up with a solution that finds a fixed number of zeros at the start of the hash. That's a trick to ensure that the calculation is sufficiently difficult, for reasons I'll get to in a moment. There's no short cut to this process, dependent as it is on sheer brute mathematical force. This is what is called a 'proof of work', to show that the miners have been through the necessary work involved in finding a solution. The proof of work is the third piece of mathematical/cryptographic wizardry involved in bitcoin. The miners throw numbers at the problem until one of them sticks and a solution is found. (Hence the mining metaphor, the idea that they're digging for the money.) This solution is then broadcast to the entire network.

At the point when the transaction is broadcast to the network, Satoshi did another clever thing. One of the problems faced by cryptocurrencies is the ‘double spend’ problem. A bitcoin is just a string of numbers: how can you tell that Joe, the customer in your coffee shop, hasn’t just cut and pasted the numbers he’s already used four times today? Bitcoin solves this by having the whole network check the entire register every time a new block is added. When the winning miner broadcasts the block, the computers on the network run through it to check that all the transactions on it are legit, and that no bitcoin has been double-spent. They in effect vote on the legitimacy of the transaction, and once the transaction is accepted, it is stamped with the number of the block and added to the blockchain. The miner who found the correct solution is compensated for their work in bitcoin: they are paid in the currency, for the work they do in validating transactions in the currency. This was another brilliant piece of design on the part of Satoshi, creating an incentive, inside the network, for people to take part in making the network run.

The mathematical sophistication of bitcoin brings with it a couple of compromises. One is what’s known as the ‘51 per cent problem’. OK, so in principle nobody can double-spend, because the blockchain checks every transaction and votes on it. But what if the bad guys were to get control of 51 per cent of the computing power on the network at any given moment? Then they could validate any transaction they wanted. There would be no way of stopping them doing anything they felt like doing with fake and double-spent coins. There’s no real solution to the 51 per cent problem, other than the sheer size of the network, which is unreassuring, as if a bank were to say that the only thing which stops criminals emptying your bank account is not some absolute principle of safety, but just that doing so would be too much effort. This is a difficulty, and one which stands out all the more given the sophistication with which Satoshi solved so many of the other conceptual problems of the new currency.

Another hard thing to ignore is the amount of energy used by miners. As bitcoin has got more popular – not civilian-popular, but nerd-popular and cutting-edge-capitalist-popular – the mining process has had more and more computer power thrown at it. The process is wasteful, since most of the mining, most of the time, is by definition unsuccessful, because only one miner wins the race. As Vigna and Casey point out in *Cryptocurrency*, by the middle of 2014, the bitcoin network, which

> was then producing 88,000 trillion hashes every second, had a computing power six thousand times the combined power of the world’s top five hundred supercomputers ... And just two and a half months later, it had almost trebled to 252,000 trillion hashes. The world has seen nothing like this level of computational expansion. That’s why some doomsayers are predicting that if bitcoin continues on its present path, the planet faces an environmental catastrophe.

The amount of energy used by the computers attached to the network can't be sustained. This is some way off, but there's no denying that the process of mining is inherently wasteful. (Bitcoin miners have a preference for setting up in places where it's cold, to cut down on their air-conditioning bills.)

There will only ever be 21 million bitcoin: the finite nature of the currency was Satoshi's way of making sure that, unlike the fiat currencies that governments are free to abuse, nobody could ever destroy the value of bitcoin by arbitrarily deciding to create more of it. The schedule is for these bitcoin to be created over the course of 130 years. As more computing power is added to the network, it becomes necessary to make the mathematical challenges harder, to slow down the miners' progress. That's where that string of zeros at the start of the proof of work comes in handy: changing the number of zeros immediately affects the difficulty of the calculation, to slow down the mining of the coins. But this does mean that an awful lot of energy is going to waste. It's an ugly side effect to a system of great intellectual elegance.

*

The result has been success for the currency, a much bigger success than most people who've never heard of it might suspect. The total value of all the bitcoin in circulation, as I write, is £4.24 billion. That number changes, often with disconcerting rapidity, since the price of bitcoin is sharply variable. This puts outsiders off, since one of the most basic functions of money is to store value; bitcoin is a lousy store of value, as many observers have pointed out. Bitcoin, however, already does an OK job with one of money's other main functions, as a medium of exchange. You can buy plane tickets, book hotel rooms, buy computer equipment, food and pretty much anything else with bitcoin, which is now accepted by tens of thousands of businesses. Indeed, since you can buy gift cards with bitcoin, and use the cards at Amazon and other e-commerce sites, you can in effect buy anything you want using the cryptocurrency. There are even bitcoin cashpoint machines. I went to look at one the other day, in a café in Bermondsey. The 'SatoshiPoint' was at the back of the premises, past the blackboard where a flat white was labelled a 'Fat Wife', past the cats'-cradle of outstretched hipster legs and MacBook Air charging cables, past the merchandise table of coffee mugs with the slogan 'Underneath your tattoos you're still a mainstream cunt.' The SatoshiPoint was broken. *Tant pis*, as Satoshi would say, if he/she/they were French, which he/she/they probably aren't. It doesn't alter the fact that bitcoin has done very well for a form of money only seven years old, with no entity backing it other than lines of code running on a network of computers.

The growing utility of the currency has attracted attention. Citizens of countries such as Argentina, whose governments have a near perfect track record of debasing their own currency and destroying the savings of their citizenry, have shown signs of preferring bitcoin to their own state's money. One of the liveliest case studies in Nathaniel Popper's brilliant *Digital Gold* concerns Wences Casares, a highly sophisticated (and very successful) Argentine investor whose interest in bitcoin comes from his up-close-

and-personal view of a broken fiat currency.[4] Casares is a big investor in and evangelist for bitcoin, not (or not only) because it will make him rich, but because it seems to him genuinely preferable to state-backed fiat money. He's not the only one.

The mathematical sophistication and philosophical suggestiveness of bitcoin are not, however, the whole story. An effectively anonymous, untraceable way of moving money: gee, hmmn, I wonder who'd be interested in that? It's no surprise that the first big-business application of bitcoin came in the form of a criminal enterprise. Satoshi Nakamoto's paper was published in October 2008. The detailed workings of the new currency, including the code which would operate it, were published on 3 January 2009. The first ever transaction made with bitcoin was a deliberately experimental, avant-garde purchase of a pizza, for 10,000 bitcoin, made on 22 May 2010. (The community marks the anniversary of the first transaction by celebrating Bitcoin Pizza Day. At current values, that pizza cost £2.77 million.) The first large-scale criminal application for bitcoin began life months later, early in 2011.

*

Silk Road was an online drug market, set up by a charming, handsome, 26-year-old Texan called Ross Ulbricht. Ulbricht, who has an undergraduate degree in physics and a master's in materials science and engineering, was (is) a strange, very 21st century combination of driven and feckless. He was not the first and will not be the last person to be led astray by a dream of the internet start-up route to billions. While doing his second degree, Ulbricht contracted a bad case of Austrian School economics, and become convinced that government and taxation were essentially coercive systems. (This revelation occurred while he was attending Penn State, a publicly funded university.) So – to fast forward slightly – he set up an online exchange where buyers and sellers could meet to trade anything that did not involve doing harm to others: what that meant in practice was no to child pornography, but a big yes to fake IDs, guns and, especially, drugs. The exchange was accessible only via Tor, the highly secure internet browser which hides the location of users so successfully that it is a great favourite of terrorists and paedos. (You may be wondering: who could possibly have created such an evil piece of software? Answer: the US navy. It invented and indeed maintains Tor as a means of communicating with spies and informants, and a tool for dissidents in totalitarian regimes. The next time you hear a securocrat talking about the need to expand internet surveillance, you may find yourself wondering why our allies invented, distributed and continue to support the single most effective web tool for terrorists, criminals and paedos. The answer is that the security classes think the usefulness of Tor outweighs the harm it causes. Except that perspective often seems to escape our leaders when they're talking about the need to spy on us.)

Tor gives anonymity and geographical unlocatability to all its users; bitcoin gave an anonymous, non-locatable way of transferring payment. The result for Silk Road, which combined the two, was explosive growth. Within two years, Silk Road was one of the most successful internet enterprises in the world, and had attracted a buyer willing to offer $1 billion. The man running it went by the pseudonym Dread Pirate Roberts, an attempt by Ulbricht to imply that the person behind the site had changed over time, since in *The Princess Bride* the identity of the DPR is handed down from one incumbent to the next. In 2013 Dread Pirate Roberts told a reporter in an encrypted internet chat that he now thought the site was worth ten or eleven figures. If his business had been legal, that estimate probably would have been accurate.

Ulbricht had, however, made a mistake. Once, and only once, in the early days of Silk Road, he had used his real email address in a forum discussion which clearly showed his involvement in running the site. He realised and quickly deleted the post, but it had already been archived, and so when the Feds came looking, they found the email address, giving them a prime suspect for DPR. By now Silk Road was a flagrant, brazen taunting of the US legal system. ‘Every single transaction is a victory,’ DPR announced, over the ‘thieving murderous’ state. DPR had a book club. It featured lots of Austrian School economics. He was in favour of a world in which ‘the human spirit flourishes, unbridled, wild and free!’ ‘Once you’ve seen what’s possible, how can you do otherwise? How can you plug yourself into the tax eating, life sucking, violent, sadistic, war mongering, oppressive machine ever again? How can you kneel when you’ve felt the power of your own legs?’ Elevated sentiments, but in reality Ulbricht was paranoid, terrified, and had even gone so far as to commission assassinations of potential informers. One of the would-be murderers was an FBI plant. The other commissioned killing had an unknown outcome, because nobody seems to have been murdered: the most likely explanation is that somebody or bodies pretended to be hitmen in order to con Ulbricht out of money. (Neither case has come to trial.) Dread Pirate Roberts had completely lost his marbles.

That didn’t make him any easier to catch. It’s not that Ulbricht nearly got away with it: he didn’t. He was nonetheless hard to pin down, because, even once the Feds knew who he was and what he was doing, that combination of Tor and bitcoin was still powerful. To convict him they would have not just to catch him at it, but to grab the computer out of his hands while he was in the middle of criminal activity. Otherwise there would be no way to link him with the activities on Silk Road. ‘Put yourself in the shoes of a prosecutor trying to build a case against you,’ DPR said in an online chat. ‘Realistically the only way for them to prove anything would be for them to watch you log in and do your work.’

Ulbricht had set up a system whereby simply closing his computer would permanently encrypt his hard drive. He could do the same just by hitting a couple of keys. They would have literally to snatch the machine out of his hands before he could so much as touch the keyboard. The Feds would have one chance and one chance only to catch him, and they would have to grab him at his computer while he was logged in as DPR and running Silk Road. So that’s what they did. On 1 October 2013 Ulbricht was sitting in a public library in San Francisco, logged into Silk Road via the library’s wifi. He was in an online chat with an FBI agent whose job was to make sure Ulbricht was still online when his colleagues swooped. Ulbricht was at a desk across from a slight young Asian woman when a couple of typical San Francisco street people began arguing loudly just behind him. He turned to look, and the young woman grabbed his laptop: she was an FBI agent. So were the street people. Nice one, the Feds. Ulbricht was logged into Silk Road under the account '/Mastermind'. Game over for Dread Pirate Roberts. Ulbricht went on trial in 2015, was convicted, and is serving two life sentences without the possibility of parole.

There are several morals to this crazy, sad, fascinating story, brilliantly told in two long pieces of *Wired* reportage by Joshuah Bearman, and also in *Digital Gold*.[5] From the bitcoin point of view, Silk Road was evidence for the largely but not entirely true maxim that there is no such thing as bad publicity. The first thing many outsiders heard of bitcoin was the collapse of Silk Road. You might have thought that the connection between the new kind of money and the new kind of criminal enterprise was off-putting, but it didn't work like that, mainly, I think, because the scandal/disaster of Silk Road contained a nugget of public relations magic for bitcoin: it showed that the currency has value. You could use bitcoin to buy and sell actual real world things that people want, stuff like cocaine and handguns and fake driving licences. If the money was good to buy those things, it would be good for other stuff too.

This speaks to the first and loudest and most persistent doubt most civilians have about bitcoin: why on earth it has any value at all. The truthful answer – which concerns the arbitrary basis of all monetary value – tends not to reassure sceptics. What Silk Road provided was a proof which went beyond argument: it showed that it just does, OK? This point was all too convincing for some of the officials involved. In a twist which would seem too rich in a work of fiction, two of the agents who hunted DPR, Secret Service agent Shaun Bridges and DEA man Carl Force (!) turned out to have stolen bitcoin from DPR. They pleaded guilty to charges of money laundering and obstruction of justice. Force got 78 months and Bridges 71. Even federal agents fell victim to the siren call of the anonymous currency.

In the process of arresting Ulbricht and shutting down Silk Road, the FBI became one of the world's larger owners of bitcoin, because it seized the site's considerable assets: 144,000 bitcoin, worth £43.9 million at today's prices. It was a point of interest what it would do with them, and a point of danger, too, since it seemed possible that once the new currency had the attention of the authorities, they might conclude that this extra-governmental, anonymous, untraceable money was, in and of its own nature, illegal. Instead, what the FBI did, after thinking for a bit, was what it does to other confiscated assets: auction them off. The implicit point was not missed: the Feds say bitcoin is legal. It follows that bitcoin has legitimate uses. That was a strong message. Bitcoin emerged from Silk Road in better shape than ever.

*

The next big scandal to affect bitcoin could and arguably should have been more damaging. It concerned an online exchange, based in Japan, called Mt Gox. (The name comes from the site's previous existence as a trading forum for the nerd-beloved trading card game *Magic: The Gathering*. It's an acronym of *Magic: The Gathering* Online

Exchange.) Mt Gox came into being as the answer to the question, how can I get hold of some bitcoin, and/or how can I turn this bitcoin I have into real money? It was the place where you could buy bitcoin at the prevailing rate of exchange with whatever currency you held. It would store those bitcoin for you. As and when you chose to exchange them for cash, it would find a buyer. There were other places where you could do that, but Mt Gox was by far the biggest and best known: by 2013, it was handling 70 per cent of all bitcoin transactions.

Mt Gox was located in Japan, and was run by a Frenchman called Mark Karpelès. He had the background characteristic of many cutting-edge computing types, combining advanced mathematical skills and a high degree of social isolation. The early bitcoin world was convivial, with many conferences and meet-ups, at which the community of early adopters, an evangelical crowd, would hang out together and exchange ideas. Everybody knew everybody. Karpelès didn't go to these gatherings. He had an unusually close relationship with his cat, Tibanne, whose health was not robust. Tibanne needed special injections which only Karpelès was able to give, and that made him unable to travel to meet-ups.

Karpelès had a clear vision of how important bitcoin could become: while running Mt Gox he was designing a point-of-sale machine, like a credit card reader, which would accept the currency; he was also working on a bitcoin café in Tokyo, which would be a showcase and proof of concept for the currency. But Karpelès, along with his skills and his ideas, had something else, too, a trait apparent in many star players from the digital world. He had very little sense of what he could not do. He didn't understand limits and practicalities. It is difficult to do ingenious new things with digital ones and zeros, and the people who have done so are correctly aware of how clever they are. But it is even more difficult to do clever things which are not digital. The digital stars dislike and resent the intractability of the non-digital world, full as it is of competing interests, resentful incumbents and human challenges. Mark Zuckerberg at Facebook tells his employees to 'Move fast. Break things.' Those maxims are much more useful when you're dealing with digital bits than when you're dealing with people. The generation of digital 'disruptors' and innovators have a shared tendency to imagine that they have important insights into worlds they don't in fact understand.

In the case of Mt Gox, the problem was basic: Karpelès couldn't run a company. Mt Gox's employees were on the second and fourth floor of a Tokyo office building. Karpelès's office was on the eighth floor. The employees often had no idea what their boss was doing, and since he kept a tight hold of the main functioning of the business, that meant nobody knew what the hell was going on. That mattered, because it became clear in 2013-14 that something was awry inside the world's main bitcoin exchange. Transactions were notoriously slow. Bitcoins being held on the exchange were worth $100 more than bitcoins elsewhere. That's because if you had money at Mt Gox, it took so long to get hold of it that it was easier to turn the money into bitcoin, and then transfer the bitcoin elsewhere: the mismatch between supply and demand drove up the price, as economics teaches us it will. There had always been problems with the Japanese bank that handled Mt Gox's transactions, but these difficulties seemed to go deeper. Nobody really knew what was going on, apart from Karpelès, and he wasn't telling.

On 7 February 2014, Karpelès suddenly closed down all transactions on Mt Gox. He put out a statement blaming a flaw in the bitcoin protocol that allowed users to alter transaction codes in a manner that made it impossible to tell if the transaction had gone through. That would enable them to spend money twice – which was exactly one of the technical problems Satoshi had supposedly eliminated with the creation of the blockchain. There was a huge backlash from the bitcoin community at Karpelès's announcement, because it turned out this 'quirk' in the protocol was well known to developers, and all the other exchanges had developed ways of working around it. Hackers began using the newly publicised flaw to attack bitcoin exchanges.

The flaw was a red herring. The real problem facing Mt Gox was, quite simply and shockingly, that it had lost all its bitcoin. To understand how this can happen, you need to grasp that when you own bitcoin, you don't own anything physical: what you own is an entry on the register. Your ownership is merely access to that entry on the register. As for 'you', in this context all you are is an address on the register: that's why bitcoin is anonymous. The address, which is nothing more than a string of numbers, could belong to anyone. To get access to it, you need its key: another string of numbers, cryptographically matched to that specific bitcoin address. So the address is one string of numbers, held publicly on the register; the key is another string, held privately by the bitcoin's owner.

The analogy with a physical key, however, is not complete. Lose a house key and you can ask your neighbours for the spare you thoughtfully gave them, or call a locksmith, or break in through a side window. Lose a cryptographic key, and you have irrevocably lost access to your information. That string of numbers is unforgiving. The history of bitcoin has some happy surprises, such as the story of the Norwegian electrical engineer who bought $26.60 worth of bitcoin in 2009, then forgot all about them until he saw coverage about the cryptocurrency in 2013. He couldn't at first remember the password he had used to encrypt his private key (that must have been a sweaty few moments) but then he did and the coins were still there. They'd gone up a bit: to $886,000. He took a fifth of them and bought a flat in a posh bit of Oslo. That's a happy ending. But the unforgiving power of the public address/private key combination has also seen 7500 bitcoin lost under a landfill outside Newport in Wales, when an IT worker chucked out an old hard drive on which he had stored the private keys from his 2009 bitcoin stash. Current value of loss: £2.1 million.

Satoshi's idea had been for people to keep their bitcoin keys in a 'wallet', a private digital locker. You'd go online when you needed to spend something from the wallet, but otherwise it would be stored safely on your computer or mobile phone or whatever. The disconcerting power of the address/key combination, though, led people to want another solution to keep their keys safe – and that, ironically, led them towards places such as Mt Gox, or indeed Cryptsy, the roughly similar exchange which collapsed in January in very similar circumstances. By similar circumstances I mean: they lost a lot of bitcoin and don't know how. The bitcoin were supposedly in ‘cold wallets’ – i.e. offline wallets – which ought to have meant they were safe. The proprietor of Cryptsy posted this message on the company blog:

> A very interesting fact here, however, is that those bitcoins have not moved once since this happened. This gives rise to the possibility they can be recovered. In fact, I’m offering a bounty of 1000 BTC for information which leads to the recovery of the stolen coins.
>
> If you happen to be the perpetrator of this crime, and want to send the coins back no questions asked, then you can simply send them to this address:
>
> 1KNi4E4MTsF7gfuPKPNAbrZWQvtd QBTAAa

There’s something sweet about asking someone who has stolen lots of money – 10,000 bitcoin, worth £2.8 million – to pretty please just give it back, and you promise not to be cross. But there’s something completely idiotic about it too. From the same blog post: ‘Some may ask why we didn’t report this to the authorities when this occurred, and the answer is that we just didn’t know what happened, didn’t want to cause panic, and were unsure who exactly we should be contacting.’ The note of bafflement is embarrassing. It’s as if it had never occurred to the masterminds at Cryptsy that a deregulated currency, explicitly constructed to be outside state control and policing, might tempt thieves, and might also mean they’d have a problem getting help from the authorities. As for the precise particulars of what happened to Mt Gox’s bitcoin, we’ll probably have to wait for Karpelès’s trial to find out: in August 2015 he was arrested by the Japanese police and in October he was charged with embezzlement.

The two best books on bitcoin itself are Vigna and Casey’s *Cryptocurrency* and Popper’s *Digital Gold*. Vigna and Casey are excellent on the technical background to the currency, the detail of how it works. They convincingly explain the trajectory of thinking most people follow when they hear about the currency, from Disdain through Scepticism, Curiosity, Crystallisation and Acceptance. Their book leaves you thinking there is a bright future to this cryptocurrency lark. Popper’s book is fascinating on bitcoin’s history, telling the stories of both the true believers and the early adopter-investors, but not sparing specifics on the many scandals and panics bitcoin has already gone through in its short life. The effect of reading both books in succession is to hear first the reasons bitcoin is full of potential, and then the reasons it is full of risks. One of the most off-putting strands in Popper’s book concerns the all too present threats of hacking, extortion and theft. The Mt Gox scandal has been the worst of these so far, but there will certainly be more to come.

There was an example of the kind of risk involved in dealing with the currency in March 2014, when Satoshi’s real identity was erroneously ‘revealed’ by *Newsweek*. Their mistake, hilariously, was to pick a real Japanese-American man called Satoshi Nakamoto, who called the currency ‘bitcom’ and told reporters, accurately, ‘I got nothing to do with it.’ He then offered an exclusive interview to the first person who would buy him lunch. It became rapidly and irrevocably clear that Satoshi wasn't, you know, Satoshi.

Before the mistake was exposed, though, many bitcoiners pointed out what a dangerous position the magazine might have put Satoshi in. If he were the cryptocurrency's creator, he would also be the owner of many early minted bitcoin. His holdings could, and likely would, be worth hundreds of millions of dollars. The key to those holdings would be kept somewhere – probably at his house. All a thief or extortionist would need to get hold of roughly half a billion dollars was that string of numbers. Bad men have been tempted to do bad things by much smaller incentives than that. This is one of those times when the people advocating for something end up being unwitting advocates for the other side of the argument. Wences Casares, the Argentine investor described by Popper, is an impressive advocate for bitcoin. And yet this detail stuck with me: he and his co-investors store their bitcoin keys in an offline laptop stored in a safe deposit box. No other form of computer storage is sufficiently secure. If those are the lengths you have to go to in order to defend yourself from crooks, what does that say about the safety of the cryptocurrency?

*

This history of criminality, fraud and disaster might well, you'd have thought, add up to a story of failure. It hasn't. In parallel with the high-profile, front-pagey things that have gone wrong with bitcoin there has been a consistent trajectory of growth and increasing interest. For all the things that have gone wrong, the currency itself has not collapsed, and has not been shown to be mathematically or conceptually flawed. The fact that the world is full of crooks, thieves, con men and incompetents doesn't invalidate the use of other types of money, so why should it invalidate bitcoin, just because it has so many criminal-friendly features? That seems to be the thinking. In any case, this currency, which is based on nothing more than mathematical calculations, is now worth billions of dollars, and has moved a long way from the early-adopting internet libertarian fringe of its early supporters. The irony is that success has brought the biggest dangers yet to the continuing existence of the cryptocurrency.

The first of these threats comes in the form of what nerds call 'forking'. The whole point of open source software, such as bitcoin, is that it is released into the wild, and users are allowed to amend and tweak it as they see fit. If a version is changed so that it becomes in some respects incompatible with other versions, that form of the software is said to be 'forked'. The software which runs Amazon's Kindle e-reader, for instance, is a forked version of Google's open source Android operating system. (It is, to use one of my favourite tech terms, a 'forked Android'.) The open source nature of bitcoin has meant that the community can make changes to it, and that these changes are in effect voted on: bitcoiners either download and use the software, or they don't. It's a kind of ongoing plebiscite. When problems have arisen, they were adjudicated first by Satoshi him/her/it/themselves, and then after he/she/it/they stopped being directly involved in running the cryptocurrency in 2011, by a small group of five 'core developers' led by a computer scientist called Gavin Andresen.

What's happened now is that there is a split in the bitcoin community, and also among the core developers. The issue is a recondite one concerning the block size – the amount of data in those ten-minute blocks of transactions. Satoshi set a block limit of one megabyte, apparently with the intention of having it rise over time as the size of the network, number of transactions and power of ordinary computers grew. One part of the community thinks that limit is about to become a crisis for the currency, which will grind to a halt as transactions have, in effect, to queue to be added to the blockchain. At that point, the currency becomes useless. So a group of developers, including Gavin Andresen, launched Bitcoin XT in August 2015, which is bitcoin as we know and love it but with a larger block size. Another group of developers disagrees: they think the change will take bitcoin too far in a corporate-friendly direction, and would prefer a smaller, slower, ideologically purer version of the cryptocurrency. The dispute has been acrimonious, and has seen a huge hacking attack launched against the XT network, and all mentions of XT censored from official bitcoin forums. So bitcoin is now forked. Mike Hearn, one of the people behind XT, quit the bitcoin world in January as a result of the split, and now regards the currency as a failed experiment. 'Despite knowing that bitcoin could fail all along, the now inescapable conclusion that it *has* failed still saddens me greatly,' Hearn wrote in a strongly felt, strongly argued blog post. Bitcoin will either recover from this, or not.

It should also be said that some bitcoiners believe more in the technology than in its use as money. David Birch is the author of a fresh, original and fascinatingly wide-ranging short book about developments in the field, *Identity Is the New Money*.[6] His is the best book on general issues around new forms of money, and new possibilities generated by blockchain technology. You finish his book convinced that something is happening in which the register, and credit more generally, and money, and banking, and identity, are all starting to blur together. That said, he's not sure about bitcoin the currency. 'I'm not convinced that money or payments is the optimum [use] of the technology,' Birch said, in response to this latest kerfuffle. It's easy to see the force of that, given that even in bitcoin's pristine form, it takes ten minutes for a block of transactions to be compiled and sent to the network for verification and adding to the chain. There is something very unmoneylike about that inherent delay and inherent complication. Bitcoin may instead have most significance not as money but as a way of authenticating identities, exchanging contracts and executing transactions. In January, the UK government's chief scientific adviser issued a report which said that 'distributed ledger technologies have the potential to help governments to collect taxes, deliver benefits, issue passports, record land registries, assure the supply chain of goods and generally ensure the integrity of government records and services.' The possibility is that the blockchain could be adapted to do this with lower levels of friction, lower levels of cost and higher levels of security than any existing system. This may not be the blockchain in its original bitcoin form, but some other blockchain or blockchains, using subtly different versions of Satoshi's brilliant technology. It's this potential that has attracted the attention of – cue music that indicates the arrival of bad guys – the banks.

Many people in the world of finance followed the bitcoin trajectory Vigna and Casey describe, from disdain through curiosity to acceptance. Their interest is mainly in blockchains. The banks have looked into the possibility of better, faster, cheaper systems powered by blockchains, and have concluded that it's possible for these to be a source of disruption and disintermediation of their business. Alternatively, they will be another profitable thing the banks own. They prefer the second option. A number of competing syndicates, funded and largely owned by the banks, are rushing to develop and patent proprietary, finance-friendly versions of blockchain technology. A consortium called R3Cev is backed by 42 financial companies and seeks to develop what would in effect be a private blockchain; Goldman Sachs, one of the firms behind R3Cev, has also filed a patent for a private blockchain-backed currency called SETLCoin (one wag at the *FT* has dubbed it 'the vampire's quid'); Digital Assets Holdings, another blockchain company, is run by Blythe Masters, the English former J.P. Morgan executive who did more than anybody else to pioneer the credit default swap, the dazzlingly ingenious new financial instrument which was a huge success until it nearly destroyed the global financial system.[7] This is just a tiny sample, and there are many other bitcoin-related initiatives. One result is a great deal of confusion. Bitcoin was apparently a major topic of conversation at Davos this year, where there was evidently much blurring between bitcoin the currency, bitcoin the technology, cryptocurrency in general, the blockchain as in bitcoin, or the blockchain as in blockchains in general. The headline news is as follows: in the world of finance, the blockchain is definitely going to be A Thing.

Irony klaxon. The very first sentence of Satoshi's original paper reads as follows: 'A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.' It looks as if, on the contrary, those very same financial institutions are going to use this new technology to keep themselves right where they are: in the middle of every possible transaction network, extracting all the rent they can.

Bitcoin true believers are annoyed that pretty much every discussion of the cryptocurrency ends with a rhapsody about the potential of blockchains. Bitcoiners reject that idea: for them, the blockchain will never succeed apart from the currency. The trouble is, though, that in internet terms, bitcoin has already been around for quite a while. January marked seven years since the launch of Satoshi's original code. In seven years, Google, Facebook and Twitter had all become not just big companies, but fundamental parts of everyday life for hundreds of millions of people. They had become verbs. M-Pesa is about the same age as bitcoin, and handles half Kenya's GDP. Bitcoin is nowhere near that. It's time for the cryptocurrency to decide what it wants to be when it grows up. Blockchains could become merely a new technique to ensure the continuation of banking hegemony in its current form. That would be one of those final plot twists which leaves everybody thinking that although they enjoyed most of the show, the ending was so disappointing they now wish they hadn't bothered. Or, along with peer-to-peer lending and mobile payments, they could have an impact as great as the new kind of banking introduced in Renaissance Italy. That would be more fun.

[1] Duke, 144 pp., £14.99, October 2015, 978 0 8223 5999 9.

[2] Yale, 288 pp., £10.99, August 2015, 978 0 300 21249 5.

[3] Vintage, 384 pp., £9.99, January, 978 1 7847 0073 8.

[4] Allen Lane, 416 pp., £20, May 2015, 978 0 241 18061 7.

[5] Ulbricht's story may strike some readers as resonating with the Mr Chips-to-Scarface journey of Walter White. A detail from *Wired*'s reporting: when the computer was snatched out of Ulbricht's hands, he was, in addition to running Silk Road, watching an interview with Vince Gilligan, creator of *Breaking Bad*.

[6] LPP, 126 pp., £7.99, May 2014, 978 1 9079 9412 2.

[7] Masters went on to be head of the commodities business at J.P. Morgan, but left after the bank paid a $410 million fine for its role in tricking California and Michigan into overpaying for energy.

Vol. 38 No. 8 · 21 April 2016 » John Lanchester » When Bitcoin Grows Up
pages 3-12 | 11085 words

Letters

Vol. 38 No. 9 · 5 May 2016

The effectiveness of cryptography depends, John Lanchester writes, on the fact that 'there is no way' of breaking very large numbers down into factors 'other than by trying every smaller number and seeing if it fits' (*LRB*, 21 April). In fact, all cryptographic questions are questions of computational complexity: the number of resources required to solve a problem grows as the size of the problem grows. The best-known method of factoring integers necessitates a lot of time (an exponentially increasing amount of time) to execute as the size of the integer grows. But there is no mathematical theorem that says no algorithm can do better: we don't know that 'there is no way' of doing it more efficiently. Furthermore, all the underlying assumptions of 'hardness' and 'impossibility' on which modern cryptography is based are unproven (though widely believed) open conjectures. Tomorrow it could conceivably be announced that every modern cryptographic system has been broken because of a single mathematician's new insight. To be sure, there are provably unbreakable forms of encryption (some were even used successfully during the Second World War), but credit card transactions, internet traffic and bitcoin do not use them.

One might argue that this fact about cryptography – that there are so few facts – accentuates Lanchester's point that 'to believe in bitcoin', you have to take the underlying mathematics 'on trust'. Not only do you have to trust in mathematics you don't understand, you're also trusting in mathematics that has the possibility of being false.

Jeremy Kun
University of Illinois, Chicago

The value of money, John Lanchester writes, rests on our belief in its value. I'd say that it rests, rather, on our belief that others will accept it. For example, I may knowingly accept a fake coin, albeit at a discount, if I think that everybody else will think it genuine. On the other hand, I may be reluctant to accept a Scottish banknote, though I know it to be legal tender, if I expect others to be leery of it. In fact whenever notes and coins cease to be acceptable – as in hyperinflation – they cease to be money, however official the fiat; whereas there have been many times and places in which formally illegal US dollars have been very good money.

Jonathan Harlow
Bristol

Vol. 38 No. 10 · 19 May 2016

It might some day prove useful to Jonathan Harlow to know that Scottish banknotes are not legal tender anywhere – even in Scotland (Letters, 5 May). For what it's worth – which in practical terms isn't much – the status of legal tender in the UK is conferred by the Treasury, and is quite narrowly defined in terms of the obligation of a creditor to accept designated notes or coins in settlement of a debt. This status is enjoyed in England and Wales by coins (up to certain limits) and notes issued by the Bank of England. These notes are not legal tender in Scotland, though, like those issued by the Scottish banks, they are approved by the UK Parliament as legal currency.

John McGill
Quoyloo, Orkney

^ Top