BLOCKCHAIN AND TELECOMS

How will blockchain technology impact telecoms policy? **DAVE MICHELS** is your guide to this much-hyped technology and its applications

Blockchain technology is widely discussed. Depending on who you ask, it is either a foundational technology, poised to disrupt and transform a wide range of industries – or a passing fad used to move around make-believe money online. Admittedly, cryptocurrencies such as Bitcoin and Ethereum are, to date, the only large-scale, real-world deployments of blockchain technology. Nonetheless, many companies are testing and developing prototypes and launching pilot projects. Though financial technology companies are firmly in the lead, telecoms operators are also experimenting with blockchain technology. A recent report forecasts that the blockchain-for-telecoms market will grow from around $50m in 2018 to almost $1bn in 2023.[1]

Speculation aside, blockchain-for-telecoms will likely remain in an early stage of development for the coming years. As a result, it is hard to predict the regulatory and policy issues that will arise from blockchain adoption in telecoms. Such issues will inevitably depend on how blockchain technology is deployed. Given this, regulators would be wise to adopt a "watch and wait" approach. They should familiarise themselves with the opportunities and challenges of this emerging technology today, so they are prepared should blockchain become widespread tomorrow.

BLOCKCHAIN TECHNOLOGY AND SMART CONTRACTS

What is blockchain? There are three basic concepts:

- It is a system for recording a series of data items (such as transactions between parties)
- It uses cryptography to make it difficult to tamper with past entries
- It has an agreed process for storing copies of the ledger and adding new entries (also called a consensus protocol).

Blockchains can be stored in a distributed manner across many different devices, called nodes. As a result, blockchain is often referred to as a distributed ledger technology (DLT).[2] The combination of distribution and cryptography makes it difficult for any single actor to change past entries, while the consensus protocol ensures that the copies of the ledger stored by the nodes are consistent. Consequently, all participants can be confident that the ledger is accurate, without having to trust a single third-party record keeper.

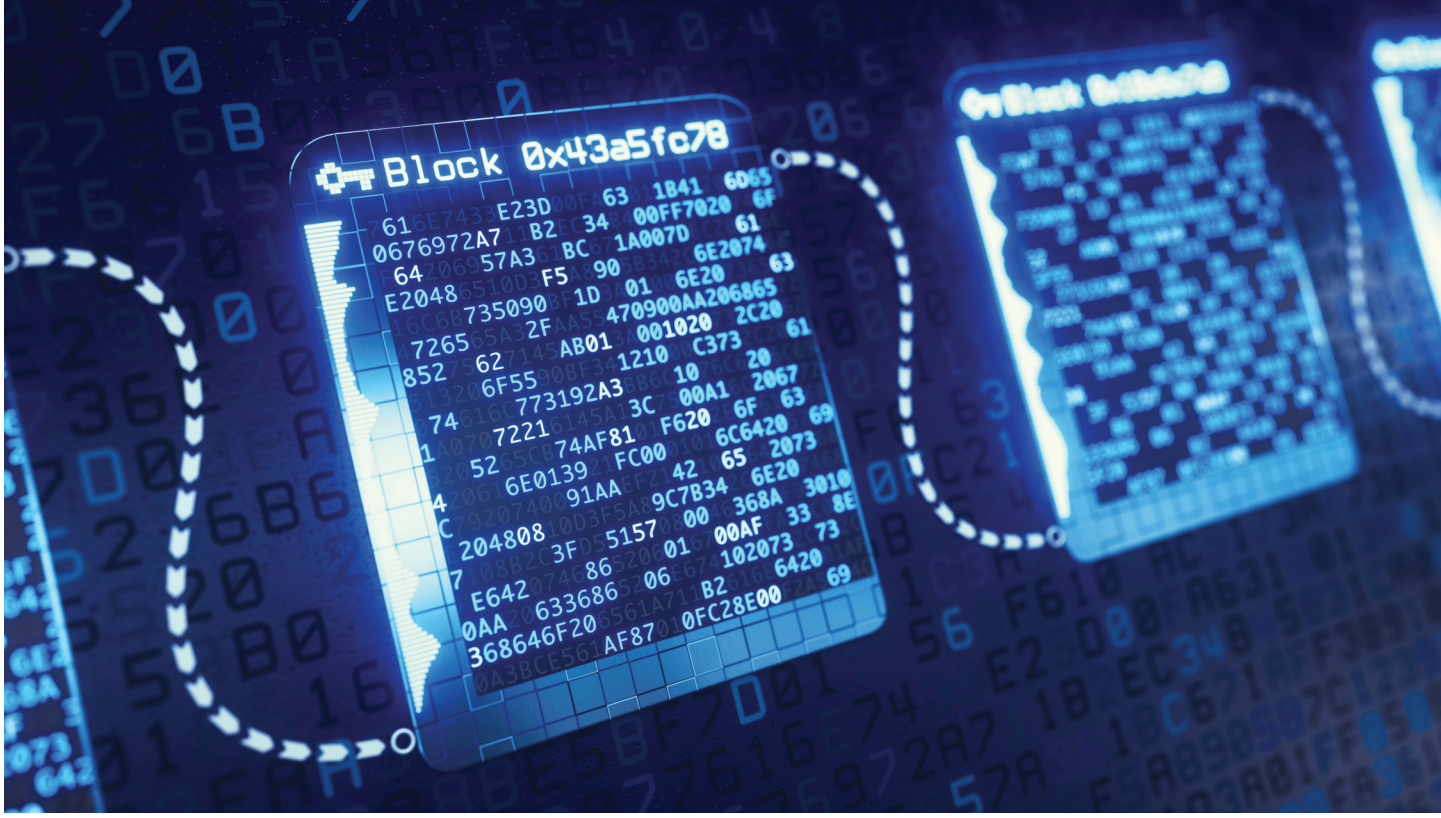
A blockchain can be used to store and record data, instead of a normal database. It may offer advantages where multiple parties need to view and append entries and are not inclined to trust a third party. By using a shared ledger, parties can avoid replicating data in separate ledgers which need to be reconciled periodically. In addition, since they are tamper-evident, blockchains can provide better proof of data integrity and transparency than ordinary databases. Further, a distributed blockchain is a resilient system, since there is no single point of failure. Even if several nodes fail, the network will continue to function.

> **"Much of the current excitement around blockchain stems from the promise of smart contracts."**

Much of the current excitement about blockchain stems from the promise of smart contracts, which are essentially computer programs that automatically bring about some specified actions, such as transferring digital assets, according to a set of pre-specified rules. As a result, smart contracts can automate agreements between parties according to a set of instructions in their code. As such, they add functionality and interactivity to blockchain applications, enabling them to perform a wide range of functions.

However, today's distributed blockchain systems have high running costs and low throughput. To achieve consistency across thousands of nodes, the Bitcoin and Ethereum networks currently use consensus protocols based on proof-of-work (PoW). This means that any participant who wants to add new entries to the ledger needs to first solve a computationally difficult puzzle (called mining). This slows down system performance and uses large amounts of energy.

In 2017, Bitcoin mining consumed an estimated 22 terawatt-hours a year, which is similar to the energy expenditure of Ireland.[3] It is also a lot more than Google consumes, which was about 6 terawatt-hours in 2015. But not all blockchain applications rely on energy intensive PoW protocols. For example, Ripple, the third largest cryptocurrency, achieves consensus through voting by a list of trusted nodes. As a result, it features lower costs and higher throughput.



BLOCKCHAIN TECHNOLOGY AND TELECOMS

Blockchain's origins lie in cryptocurrency payment platforms. The same technology could be used to support payments in telecoms. For example, in some countries, telecoms operators provide mobile payment services to their customers, such as Safaricom's M-Pesa money transfer service in Africa. In such cases, blockchain could provide an alternative back-end infrastructure.

Blockchain technology could also be used to facilitate payments and other transactions between telecoms operators. For example, since 2015, French operator Orange has invested in Chain – a company that designs private blockchain networks for telecoms. In February 2017, Japan's Softbank and US operator Sprint launched a consortium with software developer TBCASoft to develop blockchain applications. The consortium aims to provide a cross-carrier payment platform to connect carriers' back-end systems, including for wholesale roaming payments and retail top-up payments. In theory, such networks could use smart contracts to automate the execution of roaming agreements between operators, providing real-time authorisation, billing and payment. This could help prevent roaming fraud and reduce disputes between operators.[4]

Some startups are looking to go further, by using blockchain-based micropayments to fund mesh networks. For example, Ammbr aims to create a community mesh network wherein participants link dedicated outdoor routers and indoor internet access points, to provide last mile coverage. The mesh network uses unlicensed spectrum frequencies, as well as frequencies that are not used locally, such as television white space. Subscribers pay for access through blockchain-based payments, which in turn incentivise participants to install routers.[5] The resulting fixed-wireless networks could help extend outside broadband coverage to new areas (provided a fixed core network and spectrum bands are available), particularly where rollout has, to date, been constrained by a lack of operator access to capital, or by legal issues like planning permissions and wayleaves. A pilot programme will deploy Ammbr's mesh routers in Cape Town, South Africa, by the end of 2018, funded by a grant from Facebook.

Beyond processing payments, blockchain technology could also support new revenue-generating services. For example, telecoms operators could offer a digital identity service, allowing their subscribers to log in securely to third party providers' apps or on websites.[6] Such a service could be built using a private key stored securely on each subscriber's device, with the telecoms operator(s) managing the blockchain ledger that matches such keys to subscriber identities.[4] Looking even further ahead, blockchain and smart contracts could also be used to facilitate automated machine-to-machine micropayments, such as electric cars paying autonomous charging stations for power.[7]

REGULATING BLOCKCHAIN-BASED APPLICATIONS

Since Bitcoin was the first application of blockchain technology, it has shaped the public perception of what blockchain is. However, Bitcoin is best thought of as a particular implementation of blockchain technology designed for a specific use case, namely to support value transfers between pseudonymous parties without going through a trusted intermediary. It is an example of a public blockchain (also called open or permissionless). This means anybody can join the network as a node and store a local copy of the ledger.

Some worry that such public blockchains are beyond the reach of the law. Take Bitcoin – developers make the Bitcoin software publicly available as open-source software. Thousands of Bitcoin nodes around the world then download and run the software on their local machines. Now imagine you are a regulator trying to impose anti-money laundering regulations on the Bitcoin network. Who do you target with your regulation? Who do you enforce against? Fining individual node operators wouldn't shut down the rest of the network.

In some respects, the regulatory challenge is

similar to that presented by peer-to-peer file-sharing services, like BitTorrent. Software developers make the BitTorrent protocol and client software available for download. Thousands of users around the world then download and run the software on their local machines and can make their files available for others to download. Files are stored in small pieces across many different machines, instead of on centrally controlled servers. Since Napster emerged in 1999, such networks have been used for the unlicensed dissemination of copyrighted works. As there is no central party that controls the content, it is difficult to effectively prevent copyright infringement. Sending notice-and-takedown letters to individual file-sharers doesn't affect the rest of the network.

Nonetheless, courts and legislatures have found ways to regulate copyright-infringing peer-to-peer file-sharing. For example, instead of targeting individual users, many European jurisdictions require ISPs to restrict their subscribers' access to websites that index so-called magnet links to copyrighted works, like The Pirate Bay.

Generally speaking, fears of blockchain systems being somehow immune to regulation are overblown.[8] First, blockchain technology can be applied in a variety of ways to create applications with different properties. It is unlikely that the blockchain components deployed in telecoms will resemble public blockchain systems like Bitcoin. Instead, operators will use private blockchain systems (also called closed or permissioned), where copies of the ledger are controlled by a closed group of vetted participants. For example, a consortium of carriers could act as the nodes that collectively control the blockchain. They could design and manage the application so as to comply with relevant regulations.

Second, even completely open blockchains like Bitcoin are not immune to regulation. Instead, regulators can control their use by identifying and then targeting any centralised or concentrated activities within the value chain. For example, many Bitcoin users rely on intermediaries that provide an interface to the blockchain system, such as online wallets like Blockchain.info, or online exchanges like Coinbase. These services are provided by companies that can be regulated.

Thus, in September 2018, the UK House of Commons Treasury Select Committee recommended that the UK Financial Conduct Authority (FCA) be given powers to regulate crypto exchanges for the purposes of anti-money laundering and consumer protection.[9]

Finally, for particularly high-risk cases, courts could order internet service providers to perform deep packet inspection and filter out certain unwanted blockchain traffic – though this may raise privacy concerns.

In sum, there are various ways to regulate systems that use blockchain technology. Consequently, the more pertinent question is not whether regulators can regulate blockchain, but whether they should, and if so, how. It is too early to answer that question in the abstract. The specific regulatory and policy concerns will differ for each blockchain application – although some specific concerns can be foreseen.

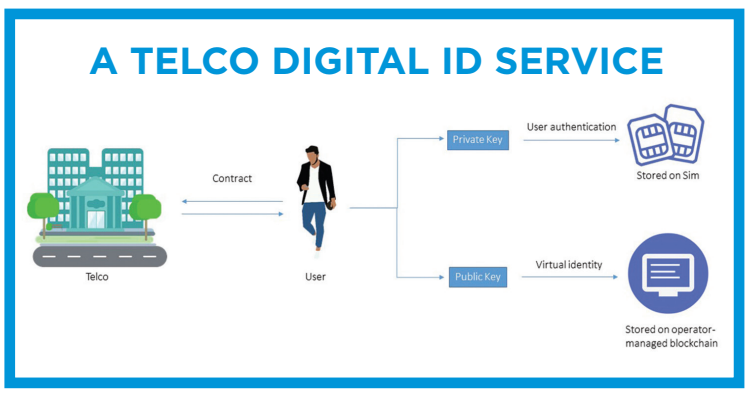
SPECIFIC CONCERN: GDPR

Any applications that process personal data will fall within the scope of relevant data protection laws, such as the EU's General Data Protection Regulation (GDPR). The GDPR has a broad reach. It applies to anyone who processes personal data and is established in the EU. It also applies to anyone outside the EU who processes the personal data of persons in the EU in the course of offering them goods or services, or when monitoring their behaviour within the EU. Personal data is a broad term: it covers any information that can be linked to an identifiable individual. This includes pseudonymised data, as well as encrypted data, as long as there are ways to decrypt it. Processing is also broadly defined: it refers to any operation or set of operations performed on personal data. So if telecoms operators provide a digital identity service for EU citizens, this activity would certainly fall within the scope of the GDPR.

> **There are concerns about how data protection rules will apply to public blockchains.**

However, there are three main concerns about how data protection rules will apply to public blockchains like Bitcoin. A first concern relates to accountability. Under the GDPR, parties who engage in data processing are called controllers or processors. Put simply, a data controller is the party in charge of the data processing operation: it determines the why and how of processing. A data processor is a supporting party: it follows the controller's instructions and processes data on the controller's behalf. Under the GDPR, the parties involved in data processing need to determine their roles as controllers or processors and agree a contract that sets out their responsibilities.

However, identifying who qualifies as a controller and a processor is complicated in public blockchain systems like Bitcoin. Software developers often only make the open-source software available for download, without processing any personal data themselves. Nodes store the ledger and process new ledger entries, but don't have any control over how the system works. Meanwhile, the users arguably



upload personal data to the blockchain when they submit transactions. So who's a controller and who's a processor? And how are all these parties supposed to conclude controller-processor agreements?

A second concern relates to international data transfers. The GDPR imposes conditions on transfers of personal data from the EU to third countries (i.e. any country outside the European Economic Area). Thus, controllers must ensure they have an appropriate legal basis for any international data transfer to a third country. Relevant legal bases include an adequacy decision from the European Commission; a certain type of contractual agreement with the receiving party; or explicit consent from the data subject. However, open blockchains are unconstrained by international borders. Anybody, anywhere, can download the ledger and start processing new blocks of entries as a node. As a result, such systems cannot exclude data transfers to third countries. Since any party in any third country can download the archive, it is difficult to see how an appropriate legal basis could be assured.

A third concern relates to respecting data subject rights. On the one hand, the GDPR aims to give data subjects rights over how information about them is processed. For example, individuals have the right to request that their personal data be corrected or deleted. On the other hand, blockchain technology purposely makes it very difficult to alter or delete any information stored "on the chain". So how would a public blockchain comply with a data subject's right to be forgotten?

While these concerns are valid, they do not apply equally to private blockchains. First, with a private blockchain, accountability for data processing can be assigned among the closed group of nodes. A consortium of carriers that operates a private blockchain system can be held responsible for complying with the GDPR. Second, to comply with GDPR rules on international data transfers, the operators would need to ensure that their system does not transfer data to third countries without an appropriate legal basis.

Third, they need to be able to comply with data subject rights, including requests for correction or deletion. Fortunately, a blockchain ledger is not technically immutable. The nodes of any given platform can "correct" their local versions of the ledger and undo specific past transactions they no longer consider appropriate.[10] They would simply move to a new version of the blockchain (called forking), and delete the old version.

Admittedly, this goes against the original aim of creating a persistent record. Nonetheless the operators of a private blockchain may agree that it is appropriate to do so to comply with data subject requests under the GDPR. Moreover, work on designing blockchains that are able to comply with data subjects' rights without forking is ongoing. Examples of promising solutions include encrypting entries and then deleting the relevant decryption keys as needed, or using so-called "off-chain" storage models.[11]

BLOCKCHAIN BITS AND PIECES

● There is a mythology about blockchain that certainly does not help its champions. The inventor of Bitcoin is supposed to be someone called Satoshi Nakamoto, who wrote the first paper in 2008, "Bitcoin: A peer-to-peer electronic cash system", and subsequently released Bitcoin software. But this is not thought to be a real person, and there has been much speculation about their real identity.

● One of the most interesting ideas for blockchain is that it is an enabler for the sharing economy and a more equitable distribution of wealth, given that one of the big challenges of the current high-tech world of globalised capitalism is "the relentless rise of inequality and the lack of steady, well-remunerated employment", as Nicolas Berggruen, chair of the Berggruen Institute, has said.

● Virtually every industry has blockchain applications mooted or implemented. They include:
– Solving problems of origin, ownership and price in the art market
– Enabling peer-to-peer fundraising donations in nature conservation and monitoring conservation (e.g. Madagascar tree-planting through Ixo's blockchain platform)
– Funding journalism, such as with Civil (see civil.co)
– Regulation of utilities, such as water in South Africa in a project involving blockchain company, Hashcash, and see the 2018 World Energy Blockchain Insights Brief, developed in partnership between the World Energy Council and PwC
– Bringing trust to the charity sector – for example Aidcoin is a blockchain system that is aiming to make donations trackable and efficient (see aidcoin.co)
– Healthcare systems are eying up blockchain for health records; Estonia already uses the technology for citizens' records
– IBM has started a blockchain practice and is working with shipping giant Maersk to use smart contracts at more than 20 ports around the world to track the movement of containers and share shipping documents.

● Applications in developing countries are attracting attention and include fundamental issues such as registering people, including children, and land; securing voting in elections (as recently trialled in Sierra Leone); and also various financial systems, including a proposal for a new mobile phone blockchain network. See bit.ly/2OkDmQ0 and bit.ly/2DhZbyR.

● The US Federal Trade Commission (FTC) has set up a blockchain working group to target fraudulent schemes which affect the agency's consumer protection and competition brief.

● The Federal Communications Commission (FCC) took action against a New York resident whose Bitcoin miner was interfering with T-Mobile's LTE network in the city.

Marc Beishon

BLOCKCHAIN: CHALLENGES AND OPPORTUNITIES

Whether blockchain will actually prove useful in facilitating cross-carrier payments or supporting digital identity services remains to be seen. Given this early stage of development, regulators would be wise to adopt a "watch and wait" approach. Pre-emptive regulation could prove heavy-handed and stifle innovation. In 2016, the European Parliament agreed to take a hands-off approach to blockchain regulation and recommended the establishment of a taskforce to monitor blockchain technology.[12] In February 2018, the Commission launched the EU Blockchain Observatory and Forum, and in October this year the European Parliament passed a resolution highlighting the

potential of blockchain and distributed ledger technologies in most sectors, including energy, transport, healthcare and education, and also in the creative industries and copyright.[13]

Nonetheless, where specific issues are likely to arise, regulators could help by issuing guidelines so as to reduce uncertainty. For example, CNIL, the French data protection authority, has released a report on blockchain.[14] In addition, telecoms regulators could establish regulatory sandboxes to test new services, as the UK Financial Conduct Authority has done for financial applications.[15] This would allow regulators to keep abreast of blockchain developments and prepare for whatever future challenges and opportunities lie ahead.

Finally, regulators could even look to take advantage of blockchain technologies themselves. For instance, a regulator could use a blockchain system to manage spectrum licences and facilitate spectrum exchanges between operators.[16] Alternatively, a regulator could request read-only access to a blockchain platform used by telecoms operators. Since the blockchain would form a reliable ledger of operator activity, access to the ledger could improve transparency and auditability. A regulator could even mandate that rules are built into the platform through smart contracts to ensure compliance with certain requirements.[17]

The Telecom Regulatory Authority of India (TRAI) has taken a first step towards using blockchain as "RegTech" to further legal and regulatory objectives. In May 2018, it issued a draft regulation that aims to reduce unsolicited commercial communications using blockchain technology. The proposal calls for operators to establish a private and permissioned distributed ledger to register customers' consent to receive commercial communications (see also box).[18] Microsoft is reportedly working with Tech Mahindra on a blockchain solution to curb spam calls, in line with the TRAI proposal.[19] If successful, a similar system could manage consent for direct marketing communications under the EU's e-privacy laws.

Further, in October 2018, the UK government awarded £700,000 to Ofcom, the communications regulator, to work with operators to develop a blockchain platform for managing and porting telephone numbers between operators (see box for details).[20] As with much else around blockchain, only time will tell whether these pioneering projects will succeed.

JOHAN DAVID MICHELS *is a researcher at the Cloud Legal Project, Queen Mary University of London, and co-author of "Blockchain demystified" in the Richmond Journal of Law and Technology at bit.ly/2SQIWNJ.*

REGULATORS CHOOSE BLOCKCHAIN FOR 'REGTECH'

The Telecom Regulatory Authority of India (TRAI) is claiming a world first in using blockchain on a large scale in the telecoms sector. The application is set out in a draft regulation that aims to curb the problem of unsolicited communications, or spam, which TRAI first started to tackle in 2010 with a "do not disturb" registry, which has a lot of subscribers – TRAI says 230 million are registered.

But the problem was not contained because "unscrupulous elements" started obtaining customers' consent, often surreptitiously, or resorted to the use of unregistered telemarketers that call or message from a 10-digit number. Recently, the incidence of fraud calls has also been on the rise.

The new regulations require that consent be explicitly recorded by a third party and be activated only after subscriber confirmation. Furthermore, the subscriber is given the option to revoke his or her consent, if it's abused or is no longer relevant.

Blockchain is the key to making it work, says TRAI, as it has proven useful where the objective is to cryptographically secure information and make it available only on a need to know basis. "Yet none may deny their actions or tamper with records, once recorded on the distributed ledger, which uniformly enforces compliance."

However, a software engineer has taken issue with the use of blockchain for this application, saying it hasn't been tested at scale anywhere in the world, and that a private and permissioned blockchain network is not secure. Shirsendu "Troy" Karmakar challenges several assumptions in TRAI's proposal in an article that can be read at bit.ly/2Qnwcws.

Meanwhile UK regulator, Ofcom, is inviting organisations to trial the porting and management of millions of telephone numbers using blockchain and ledger technology. Ofcom says about 1 billion landline telephone numbers are available in the UK, either already in use or reserved for allocation, and are issued in blocks to telecoms operators, which manage the numbers and movement (porting) of them into and out of their control. Existing systems used for this process will need to change as networks move to an all-IP (internet protocol) infrastructure and moving to blockchain has the potential to improve customer experience when moving a number between providers, lower regulatory and business costs, and provide more effective management of nuisance calls and fraud.

Says Ofcom: "Previous attempts to develop a centralised database haven't succeeded because of high costs and barriers to collaboration; but this technology offers an opportunity to build a cheaper, long-term system… We plan to share key learnings, best practices and the underlying code base with other regulators, where we can."

Marc Beishon

REFERENCES **1** MarketsandMarkets. Blockchain in telecom market worth 993.8 million USD by 2023. bit.ly/2qun6IT **2** For a more detailed explanation, see: Bacon J et al. (2017). Blockchain demystified. SSRN. bit.ly/2ALuoI2 **3** The Economist (2018).Why bitcoin uses so much energy. 9 July. econ.st/2OFtaXB **4** Monitor Deloitte (2016). Blockchain@Telco: How blockchain can impact the telecommunications industry and its relevance to the C-suite. bit.ly/2pCOU7U **5** See ammbr.com and white paper at bit.ly/2qrq6Q4 **6** GSMA (2018). Distributed ledger technology, blockchains and identity. A regulatory overview. bit.ly/2MCpgsw **7** Analysys Mason (2016). Nine blockchain opportunities that telecoms operators should explore. 13 June. bit.ly/1rq8mm1 **8** Millard C (2018). Blockchain and law: Incompatible codes? SSRN. bit.ly/2F2hVE6 **9** Commons Treasury Committee (2018). "Wild West" crypto-assets should be regulated. 19 September. bit.ly/2QKUKjB **10** IAPP (2018). Blockchain technology is on a collision course with EU privacy law. 27 February. bit.ly/2CmLZbe **11** TheNextWeb (2018). Here's how GDPR and the blockchain can coexist. bit.ly/2OhPmTz **12** EU Parliament (2016). Report on virtual currencies. 2016/2007(INI). 3 May. bit.ly/2yQLIKx **13** EU Parliament (2018). Distributed ledger technologies and blockchains: building trust with disintermediation. 2017/2772(RSP). 3 October. bit.ly/2Oj1pnb **14** CNIL (2018). Blockchain. bit.ly/2Ibed9b **15** Financial Conduct Authority (2015). Regulatory sandbox. Updated 22 October 2018. bit.ly/2z1YoyX **16** Rosenworcel J (2018). The FCC should use blockchain to manage wireless spectrum. Wired Business, 20 March. bit.ly/2DGII2M **17** Wright A, De Filippi P (2015). Decentralized blockchain technology and the rise of lex cryptographia. SSRN. Revised 25 July 2017. bit.ly/2oujvoG **18** TRAI (2018). TRAI issues the Draft Telecom Commercial Communications Customer Preference Regulations, 2018. bit.ly/2OoozUG **19** Hindustan Times (2018). Tech Mahindra, Microsoft to develop blockchain-based solution to curb spam calls. 27 August. bit.ly/2D3qb4f **20** Ofcom (2018). How blockchain technology could help to manage UK telephone numbers. 9 October. bit.ly/2QDyvLz