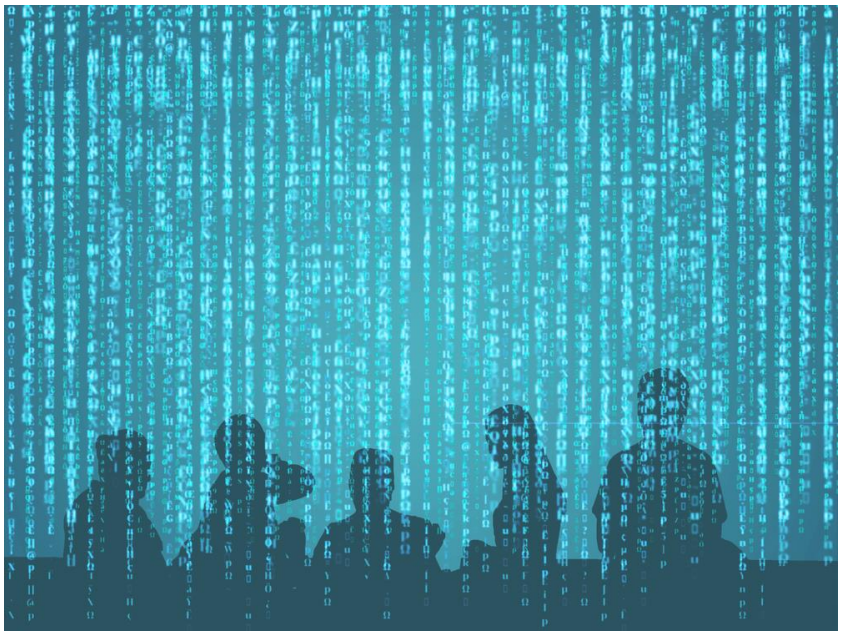
European Parliament

How blockchain technology could change our lives



IN-DEPTH ANALYSIS

EPRS | European Parliamentary Research Service

Author: Philip Boucher

Scientific Foresight Unit (STOA)

PE 581.948

.

How blockchain technology could change our lives

In-depth Analysis

February 2017

PE 581.948

AUTHORS

Philip Boucher,	Scientific Foresight Unit (STOA), DG EPRS, European Parliament
Susana Nascimento,	Foresight, Behavioural Insights and Design for Policy Unit, DG JRC, European Commission (Chapters 6-8)
Mihalis Kritikos,	Scientific Foresight Unit (STOA), DG EPRS, European Parliament (Anticipatory Policy-Making sections)

LINGUISTIC VERSION

Original: EN

ABOUT THE PUBLISHER

To contact STOA or to subscribe to its newsletter please write to: STOA@ep.europa.eu
This document is available on the Internet at: http://www.ep.europa.eu/stoa/

Manuscript completed in February 2017

DISCLAIMER

PE 581.948
ISBN 978-92-846-0549-1
doi: 10.2861/926645
QA-02-17-043-EN-N

Table of contents

How blockchain technology could change our lives

Blockchains are a remarkably transparent and decentralised way of recording lists of transactions. Their best-known use is for digital currencies such as Bitcoin, which announced blockchain technology to the world with a headline-grabbing 1000% increase in value in the course of a single month in 2013. This bubble quickly burst, but steady growth since 2015 means Bitcoins are currently valued higher than ever before.

There are many different ways of using blockchains to create new currencies. Hundreds of such currencies have been created with different features and aims. The way blockchain-based currency transactions create fast, cheap and secure public records means that they also can be used for many non-financial tasks, such as casting votes in elections or proving that a document existed at a specific time. Blockchains are particularly well suited to situations where it is necessary to know ownership histories. For example, they could help manage supply chains better, to offer certainty that diamonds are ethically sourced, that clothes are not made in sweatshops and that champagne comes from Champagne. They could help finally resolve the problem of music and video piracy, while enabling digital media to be legitimately bought, sold, inherited and given away second-hand like books, vinyl and video tapes. They also present opportunities in all kinds of public services such as health and welfare payments and, at the frontier of blockchain development, are self-executing contracts paving the way for companies that run themselves without human intervention.

Blockchains shift some control over daily interactions with technology away from central elites, redistributing it among users. In doing so, they make systems more transparent and, perhaps, more democratic. That said, this will not probably not result in a revolution. Indeed, the governments and industry giants investing heavily in blockchain research and development are not trying to make themselves obsolete, but to enhance their services. There are also some wider issues to consider. For example, blockchain's transparency is fine for matters of public record such as land registries, but what about bank balances and other sensitive data? It is possible (albeit only sometimes and with substantial effort), to identify the individuals associated with transactions. This could compromise their privacy and anonymity. While some blockchains do offer full anonymity, some sensitive information simply should not be distributed in this way. Nevertheless, although blockchains are not the solution for every problem and even if they will not revolutionise every aspect of our lives, they could have a substantial impact in many areas and it is necessary to be prepared for the challenges and opportunities they present.

This report provides an accessible entry point for those in the European Parliament and beyond who are interested in learning more about blockchain development and its potential impacts. In doing so, the aim is to stimulate reflection and discussion of this complicated, controversial and fast-moving technology. The report is non-sequential, so readers are invited to choose the sections that interest them and read them in any order. The section immediately below presents an introduction to how blockchain technology works. The subsequent eight sections each present two-page briefings about how it could be deployed in various application areas, its potential impacts, and its implications for European policy. Finally, a concluding section presents some overall remarks and potential responses to blockchain development.

How does blockchain technology work?

Before attempting to understand how blockchain ledgers work, it is worth taking a look at traditional ledgers. For centuries, banks have used ledgers to maintain databases of account transactions, and governments have used them to keep records of land ownership. There is a central authority – the bank or government office – which manages changes to the record of transactions, so they can identify who owns what, at any given time. This allows them to check whether new transactions are legitimate, that the same €5 is not spent twice and houses are not sold by people who don't own them. Since users trust the manager of the ledger to check the transactions properly, people can buy and sell from each other even if they have never met before and do not trust each other. The middleman also controls access to information on the ledger. They might decide that anyone can find out who owns a building, but only account holders can check their balance. These ledgers are **centralised** (there is a middleman, trusted by all users, who has total control over the system and mediates every transaction) and **black-boxed** (the functioning of the ledger and its data are not fully visible to its users). Digitisation has made these ledgers faster and easier to use, but they remain centralised and black-boxed.

Blockchain offers the same record-keeping functionality but without a centralised architecture. The question is how it can be certain that a transaction is legitimate when there is no central authority to check it. Blockchains solve this problem by decentralising the ledger, so that each user holds a copy of it. Anyone can request that any transaction be added to the blockchain, but transactions are only accepted if all the users agree that it is legitimate, e.g. that the request comes from the authorised person, that the house seller has not already sold the house, and the buyer has not already spent the money. This checking is done reliably and automatically on behalf of each user, creating a very fast and secure ledger system that is remarkably tamper-proof.

Each new transaction to be recorded is bundled together with other new transactions into a 'block', which is added as the latest link on a long 'chain' of historic transactions. This chain forms the blockchain ledger that is held by all users. This work is called 'mining'. Anybody can become a miner and compete to be the first to solve the complex mathematical problem of creating a valid encrypted block of transactions to add to the blockchain. There are various means of incentivising people to do this work. Most often, the first miner to create a valid block and add it to the chain is rewarded with the sum of fees for its transactions. Fees are currently around €0.10 per transaction, but blocks are added regularly and contain thousands of transactions. Miners may also receive new currency that is created and put into circulation as an inflation mechanism.

Adding a new block to the chain means updating the ledger that is held by all users. Users only accept a new block when it has been verified that all of its transactions are valid. If a discrepancy is found, the block is rejected. Otherwise, the block is added and will remain there as a permanent public record. No user can remove it. While destroying or corrupting a traditional ledger requires an attack on the middleman, doing so with a blockchain requires an attack on every copy of the ledger simultaneously. There can be no 'fake ledger' because all users have their own genuine version to check against. Trust and control in blockchain-based transactions is not centralised and black-boxed, but **decentralised** and **transparent**. These blockchains are described as 'permissionless', because there is no special authority that can deny permission to participate in the checking and adding of transactions. They can also be described as embodying social and political values such as transparency and the redistribution of power.

It is also possible to set up 'permissioned' blockchains, where a limited group of actors retain the power to access, check and add transactions to the ledger. This enables 'mainstream' actors such as banks and governments to maintain substantial control over their blockchains. Permissioned blockchains are less transparent and decentralised than their permissionless counterparts and, as such, they embody somewhat different social and political values.

1 Currencies: the vanguard of blockchain technology

While currencies are just one of several possible application areas of blockchain technology, they are by far the most popular. Likewise, while Bitcoin is just one of many currencies implemented via a blockchain, it is by far the most well-known. Many recent initiatives have focussed upon the more wide-ranging possibilities of blockchain technology, but it is rare to find any mainstream discussion of blockchain without some reference to Bitcoin or, minimally, to blockchain-enabled currencies. Since currency applications dominate discussions about blockchain and represent the most mature and well-known applications, they have great influence upon the development of blockchain technologies more broadly. Here follows a brief discussion of how blockchain applications for currencies work and some of their implications. However, since there are already several accessible guides and discussion pieces on this topic, the focus will be on how Bitcoin's dominance of the blockchain field could affect wider development of the technology and other applications of distributed ledgers.

How do they work?

Bitcoin was launched by Satoshi Nakamoto, a pseudonym for the mysterious and elusive publisher(s) of an article describing how cryptography, combined with a distributed public ledger, could be used to implement a digital currency without a central authority to authenticate payments. Traditionally, people can exchange money with those they do not know because both actors trust a third party, usually the validity of a banknote or an intermediary such as a bank or currency exchange. Nakamoto's system has no hard currency and no intermediary, but creates a trustworthy system through innovative use of cryptography and peer-to-peer networking. When one user sends Bitcoin to another, the transaction's details (such as sender and receiver addresses and the amount of funds transferred) are broadcasted to the Bitcoin network, so that the transaction can be validated by all network peers. Once it has been validated by the network, the transaction is packaged into a 'block' of transactions, and added, through the 'mining' process, to the ever-growing list of blocks that form the blockchain ledger. This list is stored by peers in the network. Bitcoin also has a feature whereby new bitcoins are generated and added to the system, having an inflationary effect. These are distributed to miners (in addition to the sum of transaction fees in the block) as a reward for successfully adding transactions to the blockchain. Mining can be done by any user with any computer, but an industry of professional miners has emerged, using dedicated computers developed especially for the purpose. The distributed structure of the system coupled with its cryptographic functionality make Bitcoin incredibly robust. The trust required to enable transactions is achieved through the knowledge that all transactions – past, present and future – are witnessed (albeit automatically) by all users.

Bitcoin is by far the largest blockchain-based currency, although several others exist with slightly different technical features. Differences are often found in the mining process, which can require substantial computing resources. For example, some currencies use less resource-intensive algorithms than Bitcoin. Peercoin's algorithm is designed to become less resource intensive as it develops. They also vary in the rate and mechanism by which new currency is generated and distributed, (therefore, in their inflation policies). Many have a predefined maximum number of coins and, once this cap is reached, no new coins will be generated and miners will profit only from transaction fees. Some currencies use algorithms that are designed to avoid the emergence of 'professional miners' that use specialist mining equipment.

Because transactions cost very little (currently from €0 to €0.10), but provide a permanent, secure record, it is possible to use Bitcoin blockchain for other non-financial purposes. This 'piggybacking' could be used to explore and launch several other non-currency-related applications from voting to patent protection. While this kind of approach prevents the developer

from implementing bespoke features that they may have introduced in their own blockchain implementation, it does provide a low-cost, readily accessible and stable infrastructure, making it an excellent 'sandpit' for exploring ideas. Other blockchain-based currencies have been set up with wider applications explicitly in mind. Ethereum is a blockchain implementation set up following Vitalik Buterin's white paper and crowdfunding campaign. It includes a currency (ether, which is described as 'fuel') and also a code that can be used to implement a wide range of non-financial functions (see smart contracts, digital rights management and decentralised autonomous organisations).

Potential impacts and developments

In 2014, a European Banking Authority opinion highlighted several risks presented by blockchain-based currencies. It also dismissed their immediate benefits – notably fast, secure and cheap transfers – as irrelevant in the EU, where conventional transfers are already relatively fast, secure and cheap. For many users, the real advantages of blockchain-based currencies lie, beyond minor time and cost savings, in the functionality and values that are not found in traditional currencies. These may include some of the well-publicised 'problems' of Bitcoin, such as its huge price spikes and use in illegal markets on the dark web, both of which may in fact have attracted many new users. Simply put, if there were no substantial benefits to using blockchain-based currencies in Europe, then there would be no substantial use in Europe. Adoption of blockchain-based currencies continues to grow, however, despite a major security breach which tested Ethereum's ideological foundations.

These currencies are already at the vanguard of blockchain development, which could lead to a major techno-social upheaval. If they fulfil their potential, they could spearhead a process of decentralisation whereby the institutions that traditionally govern finances – including governments and banks – become less powerful. On the other hand, these same governments and banks are currently driving blockchain research and development in directions that suit their own purposes. These blockchains may prove less decentralised and transparent than others.

However, perhaps the greatest impact of blockchain-based currencies will be found in other areas beyond the financial system. Bitcoin *et al* provide a wide user base, fertile spaces for experimentation and 'fuel' to propel new ideas forward. Even if Bitcoin does not revolutionise the financial system, it might well pave the way for other implementations that could offer serious benefits for supply chains and government services, for example. While discussion of a wide range of applications of blockchain are now commonplace, currencies such as Bitcoin have dominated most media and policy attention to blockchain over the past few years and this could affect the ways in which the technology develops. In other words, frequent reference to the fluctuating value of Bitcoin and its use in black markets may distract the relevant actors and public from a more productive debate about the wide range of opportunities and challenges that the technology actually presents.

Anticipatory policy-making

Blockchain-based currencies present many legal and regulatory challenges including consumer protection mechanisms, enforcement methods and possibilities for engaging in illegal activities such as tax evasion and the sale of unlawful goods. They also present several potential benefits for citizens, including reduced costs, improved security and a more accessible and innovative financial system. These and other issues were recognised in a recent motion passed at the European Parliament, which also highlighted the wider potential of blockchain technology 'well beyond the financial sector', and called for a proportionate regulatory approach and the development of appropriate capacity and expertise at EU level.

2 Digital content: blockchain and rights management

Art forgery and fraud are long-established disciplines but, in the internet age, it can be as easy as Ctrl+C. Media content has been widely copied and shared – often illegally – since domestic hi-fi systems made it easy to copy vinyl records and radio broadcasts onto cassette tape. The internet made piracy even easier. Early users organised global networks for sharing copied CDs by post. As bandwidths increased and e-formats emerged, file sharing networks brought piracy to the mainstream. Currently, media piracy is most often organised via 'torrents' and, increasingly, streaming. While the distribution of media content in this way is often illegal, the practice is so widespread and enforcement so difficult that compliance is often treated as though it were voluntary. Recently, legitimate subscription services have displaced some piracy by providing access to media while paying royalties to rights holders using revenue from membership fees or advertisements. However, no distribution model, until perhaps blockchain, has managed to respond effectively to the realities of the illegal trade in digital content in the internet age, while balancing the interests of the original author, the customer and the various intermediaries.

When consumers purchase books and discs, they come to own physical artefacts that they can later sell, give away or leave as part of their inheritance. There are limitations to their rights, for example they should not distribute copies, and should pay royalties if they broadcast the content. In buying the digital equivalent of this same media, consumers know they will not gain ownership of a physical artefact, but many do not realise that they do not gain ownership of any content either. Rather, they enter into a licensing agreement which is valid for either a period of time or a fixed number of plays. These licences cannot be sold, given away or even left as part of an inheritance. Building a collection of legitimately-owned digital music, literature, games and films often comes at a cost similar to that of a collection of various discs and books with the same content. It is a substantial lifelong investment but one that cannot be transferred and that expires on death. While older generations might take pleasure in reliving the tastes and experiences of loved ones via the boxes of vinyl, books and games they left behind, today's children may not enjoy the same access to their parent's digital content. Could blockchain technology help resolve these and other problems with digital media?

How digital rights could be managed on the blockchain

Blockchain technology could be used to manage consumer rights associated with digital products. In most cases, this will involve mass-reproduced works, the digital equivalent of CDs, DVDs and books, where the original artist sells many copies of the work. However, it is also relevant for the emerging field of unique digital artworks, which is the digital equivalent of, for instance, a painting. Here, the buyer is not purchasing a derived version, like an MP3 of a song, but exclusive rights over the original work itself. Blockchain could protect consumers and creators of digital works of all kinds by recording the ownership history of digital property and perhaps even by enforcing digital rights.

The blockchain could be used to register all sales, loans, donations and other such transfers of individual digital artefacts. All transactions are witnessed and agreed by all users. Just like transactions in a bank account or land registry, artefacts cannot be transferred unless they are legitimately owned. Buyers can verify that they are purchasing legitimate copies of MP3s and video files. Indeed, the transaction history allows anyone to verify that the various transfers of ownership lead all the way back to the original owner, that is, the creator of the work. The concept could be combined with smart contracts so that access to content can be lent to others for fixed periods before being automatically returned, or so that inheritance wishes could be implemented automatically upon registration of a death certificate. For any of this to work, it is crucial that when content ownership is transferred from one party to the next, the former owners lose their

access, just as they would if they sold a vinyl record on the second hand market. Indeed, knowledge of when one user's rights end is just as important as knowing when another user's rights begin. Here, blockchain would make it possible to check who the owner of content was, as well as its ownership history. This would enable customers to ensure that they were buying legitimate goods rather than illegitimate copies, and could also enable rights holders to enforce their rights. Checks of legitimate ownership could even be enforced through technology, with devices checking ownership against the user's profile before allowing playback. This would require the development of new codecs and industry standards, and file formats that bundle content with permissions.

Aside from buying licenced copies of digital works such as MP3 songs, it is also possible to buy and sell original works, i.e. the song itself. Just as buying a painting affords more rights than buying a copy of a painting, the buyer of original digital works also purchases the exclusive right to broadcast the content, to sell copies of it, and to take action against others that use the content unlawfully. For the buyers, it is crucial that they know whether they are buying ownership of the work itself with the associated value and rights, or merely a reproduction that was licenced for personal use. In this case, the blockchain could be used to verify the real owner of the content, whether it is the original version or a legitimate copy of it, and the set of rights that are bundled with this content.

Aside from the rights of sellers and purchasers, the blockchain could be used to protect the rights of the original creators of works, who may retain some rights after the sale of their content. These original creators may comprise a complex network of actors claiming partial ownership and entitlement to royalty payments when the content is used for commercial purposes. For music tracks, for example, this might include writers, musicians and other artists as well as recording engineers, managers and a range of specialist intermediaries. The entitlements of each of these actors, as well as the terms and means of their reimbursement can be digitally encoded, enabling more reliable and efficient payment. Royalty payments could even be executed automatically via smart contracts.

Potential impacts and developments

Using blockchain technology in this way could for the first time enable consumers to buy and sell digital copies second hand, give them away or donate them to charity shops, lend them to friends temporarily or leave them as part of an inheritance – just as they used to with vinyl and books – while ensuring that they are not propagating multiple unlicensed copies. For blockchain to succeed in underpinning a method of managing digital rights where so many others have failed, it would have to balance the rights of sellers, buyers, network of actors that comprise the original owner of the content and a huge range of other intermediaries, including those that develop and maintain the blockchain itself. With such complex networks of interests at stake, it would be idealistic to expect a quick and uncontroversial solution to emerge, although some suggest that within a timescale of 10 to 15 years blockchain technology can be expected to have had a real impact on the music industry, with more immediate opportunities for early movers.

Anticipatory policy-making

Law will continue to have an important role in identifying copyrighted works and settling disputes. Blockchain development in this area could lead to multi-territorial licensing policies and enhanced legal certainty for creators and purchasers while providing effective dispute resolution mechanisms, particularly in relation to tariffs, licensing conditions, entrustment of online rights for management and withdrawal of online rights.

3 Patents: protecting innovators while incentivising innovation

Patents give their owners the exclusive right to exploit innovations for a specific period. The patent system was designed to incentivise innovation by giving innovators a head start over their competitors to profit from their ideas. After all, why would inventors invest the time and money required to develop an idea if others could copy it and profit immediately, without contributing to the costs of development? However, protecting innovators is not the same as incentivising innovation. The patent system must balance protection of innovators against the protection of competitors. If innovators are not protected, then exposure to freeriding competition will deter investment in new innovations. On the other hand, if competitors are not protected, they would be deterred from investing in improvements and cost savings, and would maybe even be blocked from joining the market and breaking the original innovator's monopoly. At its most basic, the patent system can be seen as an exchange in which the government grants the innovators a monopoly (limited in time and scope) to exploit their innovation, and in exchange the patent holders publish details of how their innovation works, which helps others to develop improvements and alternatives.

There are several well-known problems with the patent system. For example, competitors can sometimes exploit the patent before the innovator, either because the patent was not strong enough or because the holders were incapable of defending themselves against unlawful infringements. This, combined with the expense of gaining patent protection in several regions, means that some firms prefer to take the risk of bringing their innovations to market without any patent protection at all. Another problem is identified in the complexity of the patent system. There are different policies and systems in place in different countries. Despite recent developments, there is still no unified EU patent system. Nonetheless, the European Patent Office offers a 'one stop shop' for registering patents in each Member State's system, although the cost of translations, validations and renewals in several systems makes patenting relatively expensive in Europe.

A further problem for the patent system is identified in the emergence of 'patent trolls', which do not innovate as such but acquire patents and seek damages for their infringements. While their claims do not always hold a strong legal basis, firms are often unable or unwilling to cover the legal expenses required to defend themselves, preferring to settle out of court. European competition authorities are increasingly investigating such abuse of patents, particularly in the high-tech sector.

While many aspects of the patent system are now digitised, there have been no major changes to its structure since the information revolution. It has been suggested that using blockchain instead of traditional patents could enable more fluid innovation by reducing contract disputes, and that blockchain could offer an opportunity to repair some aspects of the patent system. Here an attempt is made to explain how blockchain could intervene in the patent system and what benefits this could bring, before consideration is given to some of the more radical claims that it could substitute or even 'end' the patent system.

How blockchain could help the patent system

Two features of blockchain technology make it particularly relevant to the patent system: 'hashing' and 'proof of existence'. The first, hashing, is a process through which a document is transformed into a fixed length code which is described as a digital fingerprint or, more often, a 'hash'. All hashes are unique, and even very minor differences, such as a missing accent on one letter of a long document, would lead to a radically different hash. Only repeating the hashing process on an identical copy of the original document will produce the same hash. Crucially, it is impossible to regenerate a document from its hash. The second feature, proof of existence, involves recording

these hashes on the blockchain. In doing so, a record is created that this hash existed at a given time. The record can be verified by anybody, but nobody can interpret the content of the hash. However, holders of the original document can prove that the document existed at the time the transaction was made by repeating the hashing process on an identical copy of their original document (by using the same hashing algorithm to produce the same hash, it follows that they have the same original document). This presents the interesting possibility of publically recording the fact that a document existed without revealing any of its content. It has been suggested that innovators could use this process to protect their work by recording a hash of their patent description (or, perhaps, a piece of literature or extract of computer code) on the blockchain. Indeed, 'proof of existence' services are already available in the context of patent protection. In this case, they 'piggyback' the capabilities of larger existing blockchains, specifically the Bitcoin implementation, although a bespoke system for recording hashes could also be designed and implemented specifically for 'proof of evidence' purposes.

Potential impacts and developments

Deploying blockchain technology within the patent system could reduce inefficiencies in recoding and agreeing the time of registrations in an efficient way, perhaps across several national patent systems. Blockchain-based proof of existence services could be offered as the first step in the process of applying for a patent. From here, the process could be streamlined and secured, making the steps more transparent to the applicant, while simultaneously reducing the potential for corruption. However, while improvements in the ways in which innovations are registered and time-stamped would bring tangible benefits to the patent system, the more serious problems – such as patent trolls and the cost associated with translation – may require a different kind of response.

There have been some (mistaken) claims that a patent is nothing more than 'a concept stamped and kept in a place where it is unfalsifiable'. Indeed, it has been suggested that blockchain could replace the patent system while allowing innovators to keep their details private. However, the publication of patents is a key part of their function: the promotion of innovation. By publishing patents, competitors are encouraged to develop alternatives and improvements, which could break monopolies after the expiry of the patent, while inspiring innovations in other areas not covered by the patent. Recording who registered an idea and when is only a very small fraction of the work done by patent office intermediaries. Patent officers also assess the novelty of proposed patents, check whether they are aligned with regulations and policies in that region and publish searchable archives of accepted patents, all of this being important work that cannot be replaced by blockchain technology.

Anticipatory policymaking

Current patent systems could be made more efficient through the use of blockchain technology and patent offices could offer low-cost 'proof of existence' services. However, it must be made clear that proof of existence via a blockchain (or, indeed, any other means) cannot be interpreted as equivalent to patent protection. For proof of existence provided by third parties, such as those that make use of the existing Bitcoin blockchain, to be accepted as a legitimate means for keeping records, they would have to be recognised as such by the appropriate enforcement bodies.

4 E-voting: revolutionising the electoral system?

Despite the digitalisation of several important aspects of modern life, elections are still conducted largely offline, on paper. Since the turn of the century, e-voting has been considered a promising and, perhaps, inevitable development that could speed up, simplify and reduce the cost of elections. It has been seen as a potential means of increasing engagement and turnout, and even restoring links between citizens and political institutions, claims that should be read with some scepticism, e-voting could take many forms: using the internet or a dedicated, isolated network; requiring voters to attend a polling station or allowing unsupervised voting; using existing devices, such as mobile phones and laptops, or requiring specialist equipment. Now there is a further choice to be made: to continue trusting central authorities to manage elections or to use blockchain technology to distribute an open voting record amongst the citizens. Many experts agree that e-voting for national elections would require revolutionary developments in security systems. However, there are many other kinds of regional and organisational election that could be digitised more simply through the use of blockchain, making it simpler to involve more people in taking important decisions, adopting long-term strategies, making investments and selecting people for a wide range of positions.

How blockchain technology could be used for e-voting

The blockchain is a means of logging and verifying records that is transparent and distributed among users. Usually, votes are recorded, managed, counted and checked by a central authority. Blockchain-enabled e-voting (BEV) would empower voters to do these tasks themselves by allowing them to hold a copy of the voting record. The historic record cannot be changed, because other voters would see that the record differs from theirs. An illegitimate vote cannot be added, because other voters would be able to see that it is not compatible with the rules (perhaps because it was already counted or is not associated with a valid voter record). BEV would shift power and trust away from central actors, such as electoral authorities, and foster the development of tech-enabled community consensus.

One way of developing BEV systems is to create a new, bespoke system, designed to reflect the specific characteristics of the election and electorate. A second approach that may be cheaper and easier is to 'piggyback' a more established blockchain, such as Bitcoin. Given that the security of a blockchain ledger relies upon the breadth of its user base, this approach may also be more secure for minor organisational elections with a small number of voters and limited resources to develop a bespoke system.

The strongest potential for BEV is in organisational contexts. Indeed, they have already been used for the internal elections of political parties in Denmark and shareholder votes in Estonia. Taking the concept a step further, BEV could be combined with smart contracts, to automatically take action under certain agreed conditions. Here, for example, election results could trigger the automatic implementation of manifesto promises, investment choices or other organisational decisions.

Many analysts have considered blockchain in a supporting role for deeper transformations, for instance in discussions of virtual administrations, 'techno-democratic systems' and the more distant possibility of implementing BEV for national elections. Ambitious suggestions have raised the possibility of using blockchain to implement 'liquid' democracy, combining direct democracy (whereby citizens vote regularly on specific policy decisions) with a delegate system (whereby citizens can either vote on these specific issues themselves or assign their votes to any other citizen – be they a politician, journalist, scientist or trusted friend – and withdraw or reassign this delegation at any time).

Potential impacts and developments

Considering minor elections and organisational decision-making, BEV could help deliver a more participatory and bottom-up social structure by offering a relatively cheap and secure e-voting system. In the context of more ambitious suggestions for national elections, the stakes are much higher and the situation is more delicate. Critics have questioned the level of anonymity and accessibility offered by BEV, and raised the problem of coercion. However, while BEV may offer several advantages over paper and other e-voting systems, many of these concerns apply equally to traditional paper systems. *Coercion* is a threat for any voting system that offers remote participation (e.g. postal votes). For both BEV and paper elections, the use of private polling booths is the only guarantee against this. *Accessibility* to all voters is another key concern in all elections. Depending upon the interface, BEV might be considered too complicated for some voters, especially if the system is fully decentralised with the option to access data and check that the correct procedures have been followed. *Anonymity* is often considered a crucial element of democratic participation, although even some national elections are not fully anonymous. The UK, for instance, has a 'pseudonymous' paper voting system where a code links each ballot paper with a personal entry on the electoral registry. There, voters have no choice but to trust the electoral authorities to protect their anonymity. While it would not be easy to discover how individuals voted, it does remain a possibility. BEV is also pseudonymous, so it may sometimes be possible to discover how an individual voted. Work is in progress on a technical response to this issue in developing BEV systems that offer full anonymity. Another approach could be to trust a central authority to distribute pseudonyms for use in a BEV and to keep them secret, just as they do now in the UK's paper voting system. This would introduce a degree of centralisation into the system which may well be considered acceptable in the context of national elections.

Another key question is how to ensure widespread trust in the security and legitimacy of the system. As with paper-based elections, it is not enough for the result to be fair and valid. The whole electorate, even if they are disappointed with the result, must accept that the process was legitimate and reliable. As such, beyond providing actual security and accuracy, BEV must also inspire confidence and trust. The fact that the blockchain protocol is quite complicated may be a barrier to mainstream public acceptability of BEV.

In assessing the potential impact of BEV, consideration must be given to the values and politics it reflects. BEV does not just digitise the traditional voting process, it proposes an alternative with a different set of values and political foundations. Traditionally, authorities manage elections and the process is black-boxed, centralised and top-down. BEV is the opposite. The process is managed by the people and it is transparent, decentralised and bottom-up. While participation in traditional elections reinforces the authority of the state, participation in BEV asserts the primacy of the people. In this light, it is not surprising that links are drawn between BEV and a transition towards a more direct, decentralised and bottom-up democracy and with 'liquid' democracy as mentioned above. In any case, the extent to which blockchain technology will flourish in the area of e-voting may depend on the extent to which it can reflect the values and structure of society, politics and democracy.

Anticipatory policy-making

While organisations are broadly free to organise internal elections with blockchain if they so choose, they must comply with European law on privacy and data protection. Although European law does not specify protocols for political elections in Member States, some convergence has occurred and efforts have been made to encourage use of e-voting while respecting the constitutional principles of electoral law (universal, equal, free, secret and direct suffrage).

5 Smart contracts: if code were law

Blockchain ledgers present several interesting and novel features over centralised ledgers. However, beyond recording the time and details of transactions, they can also play a more active, potentially autonomous role in the management and implementation of transactions. By embedding code in the blockchain, transactions can be executed automatically in response to certain conditions being met, providing a 'guarantee of execution'. Self-executing smart contracts based upon this functionality are developing rapidly. Questions arise however when code and law become one.

How do they work?

While smart contracts could refer to several different concepts, their 1994 definition as a 'computerised transaction protocol that executes the terms of a contract' remains broadly useful in the context of blockchain technologies. At their simplest, the terms of an agreement between two or more parties are programmed into code (sets of instructions) that are stored on a blockchain in much the same way that transactions are routinely stored on other blockchains. When certain conditions that are described in the code are met, specific actions, which are also defined in the code, are automatically triggered. So, for example, the delivery of products could trigger an instruction to make a payment. This could, in turn, trigger other instructions in other smart contracts, perhaps to exchange currency or make orders further down the supply chain. Many of the proposed examples of near-term applications are in the finance sector, such as loans and insurance products that require substantial manual resources that could be automated. Smart contracts could be used to automate inheritance, with the distribution of assets – including media content – triggered automatically upon the registration of death.

The Ethereum blockchain features its own programming language and currency, which were set up specifically to support smart contracts. Other approaches to smart contracts make use of other blockchain implementations including Bitcoin. At this stage, smart contracts still require some initial effort and expense to set up, so they are better suited to repetitive agreements rather than one-off contracts. Given their predetermined nature, they are not well suited to situations that are subject to substantial change during the contract period. Indeed, the level of legal uncertainty would make it prudent to restrict smart contracts to relatively consensual relationships and agreements that are unlikely to be disputed by either party. Finally, since they react to digital stimuli and trigger further digital processes, they are most effective where the various clauses' conditions and consequences are also of a digital nature, and are thus well-suited to digital automation.

Potential impacts and developments

Since the blockchain ledger is immutable, the agreed code (and thus the agreed contract) can only be cancelled or modified under terms that are already allowed for in the code itself. Traditional contracts offer the choice to pay what is owed according to the contract or break the contract and face the consequences, perhaps involving legal action. However, if the payment is automated in a smart contract, the choice is no longer available, as the transaction is executed automatically.

A radical interpretation of smart contracts would reduce the contract to the code, effectively declaring the code as the law itself: self-contained, self-performed and self-enforced. This could be the position of an 'extreme' faction of the grassroots blockchain movement, effectively positioning itself as being beyond the control of established structures, such as nation states and legal jurisdictions. Where the code is treated as the law, any mistakes or accidental vulnerabilities become part of the contract too. Exploiting such bugs to take control of assets would not be

considered theft, because the error that enabled the withdrawal is part of the code and thus, by definition, within the 'law'. Smart contracts could also contain illegal clauses, such as inheritance distribution codes that do not provide for the inheritance taxes that apply in that jurisdiction.

A more realistic interpretation of smart contracts would position them within the wider legal system. Just as with paper contracts, additional requirements can be imposed, and clauses may be nullified or reinterpreted on the basis of the intention of the parties and wider law. The law of the land always sits above the 'law' inscribed in the code, even where legal proceedings and enforcement may prove difficult. As such, while most discussions of smart contracts recognise that they will provide efficiency gains in several areas, they are not expected to replace either traditional contract law or traditional contract lawyers.

Unlike simpler blockchains that record transactions, those that include executable code feature an extra dimension of complexity and agency. This means they may require more processing power to mine and maintain the system, which could translate into higher costs, including energy use. This complexity may also open blockchains to more security vulnerabilities, which, combined with the 'code as law' ideology, could create serious practical challenges for smart contracts. These problems may be less frequent as norms develop and the first generation of 'smart lawyers' emerge (i.e. lawyers who are trained and experienced in managing smart contracts).

Anticipatory policymaking

There are several areas of law that could be vulnerable to exploitation where the contract is not considered to be part of a traditional legal jurisdiction. Examples include taxation (e.g. on income, sales, inheritance and capital gains), exploitation (e.g. on rental and employment contracts) and corporate crime (e.g. price fixing and insider trading). It may be necessary to find new ways of asserting the primacy of national law in the event that the automation involved in smart contracts makes it difficult to enforce. New government responsibilities could emerge in the process of applying traditional judicial processes to smart contracts, such as arbitration when bugs are found in contract-code. As programmers start to translate agreements into executable code, they are effectively making decisions about how they will be implemented in practice, which may mean they carry greater legal responsibilities.

Smart contracts can be inflexible and unable to adapt to changing circumstances or the preferences of parties. Not all possible questions can be answered in advance, and there will always be unforeseen circumstances that require interpretation of how contract clauses should be applied. Code is simply too rigid to allow all contracts to be algorithmically determined. The adjudication of contractual disputes and enforcement of contractual clauses may present challenges as the field develops.

Traditional contract law, particularly the record-keeping requirements and evidentiary rules, may need to be modified so as take account of the automated and deterministic nature of smart contracts, as well as issues to do with their validity and enforceability. The law is expected to face challenging questions concerning the need to establish a link with the physical, perform the necessary validation procedures and ensure compliance of blockchain applications with the applicable law. Should the technical code approached through Lessig's lens be the most significant form of law? Criteria are clearly needed to ensure the legal validity and enforceability of smart contracts under the law.

6 Supply chains: transparency and accountability at last?

Global trade is based on an estimated €16 trillion supply chain sector. Goods are produced and distributed through a vast network of producers, retailers, distributors, transporters and suppliers in a complex arrangement of processes for managing contracts, payments, labelling, sealing, logistics, anti-counterfeit and anti-fraud.

The scale and complexity of the systems involved leads to high transactional costs, frequent mismatches and errors in manual paperwork, as well as losses through degradation and theft along the way. Other issues include abusive or unsafe working conditions; environmental damage through inefficacies, illegal extraction and production processes; forgery and imitation and health risks through poor supply chain management. Such problems are frequently highlighted in high-profile incidents, for example with the supply chains for food, clothing and diamonds. Some suggest that standards and certification have improved choice differentiation and consumer awareness, but the actual processes remain costly and unreliable, especially in regions with high levels of corruption. Full 'chains of custody', which prove the origins of each product or material, are still fragmented across organisations and vulnerable to fraud and error, even between certified companies. There is a growing call for safer, more trustworthy and transparent supply chains of goods and services. The question is whether blockchain technology can really improve today's supply chains and logistics sector to respond to operational inefficiencies, fraud and perhaps even some 'grand challenges' such as unethical labour practices and environmental degradation.

How supply chains could be managed on the blockchain

Blockchain-based applications have the potential to improve supply chains by providing infrastructure for registering, certifying and tracking at a low cost goods being transferred between often distant parties, who are connected via a supply chain but do not necessarily trust each other. All goods are uniquely identified via 'tokens' and can then be transferred via the blockchain, with each transaction verified and time-stamped in an encrypted but transparent process. This gives the relevant parties access whether they are suppliers, vendors, transporters or buyers. The terms of every transaction remain irrevocable and immutable, open to inspection to everyone or to authorised auditors. Smart contracts could also be deployed to automatically execute payments and other procedures.

Potential impacts and developments

Several companies, innovators and incumbents are already testing blockchain for record-keeping in their supply chains. Everledger enables companies and buyers to track the provenance of diamonds from mines to jewellery stores and to combat insurance or documentation fraud. For each diamond, Everledger measures 40 attributes such as cut and clarity, the number of degrees in pavilion angles and place of origin. They generate a serial number for each diamond, inscribed microscopically, and then they add this digital ID to Everledger's blockchain (currently numbering 280 000 diamonds). This makes it possible to establish and maintain complete ownership histories, which can help counteract fraud and support police and insurance investigators tracking stolen gems. It also allows consumers to make more informed purchasing decisions, e.g. to limit their search to diamonds with a 'clean' history that is free from fraud, theft, forced labour and the intervention of dubious vendors who are linked to violence, drugs or arms trafficking.

London based social enterprise Provenance has developed a real-time data platform that gathers and verifies the origin of an asset by assigning it a token or 'digital passport' that can be tracked

throughout the whole supply chain until it reaches its destination. This could be useful in counteracting fraud in the sale of goods with protected designations of origin, such as those often awarded to regional specialties, such as wine and cheese. SmartLog builds smart contracts into shipping containers to track their location and surroundings for resource planning. Blockchain is also being used to minimise risk in payments, with companies such as Skuchain and Fluent offering blockchain-based support for supply chain financing and payments. Another project is developing a system to streamline the manual processing of documentation, making use of a private blockchain to share information between exporters, importers and their banks. Wal-Mart, the world's largest retailer, is trialling Blockchain for food safety. It is expected that a Blockchain-based accurate and updated record can help to identify the product, shipment and vendor, for instance when an outbreak happens, and in this way get the details on how and where food was grown and who inspected it. An accurate record could also make their supply chain more efficient when it comes to delivering food to stores faster and reducing spoilage and waste.

Blockchain-based systems have the potential to enhance the efficiency of procurement, logistics and payment processes, reduce manual processing of import/export documentation, ensure conformity and delivery of goods and prevent losses, thus generally reducing costs, improving safety and security, and minimising fraud. They can also provide the means to verify the authenticity, origin and ethical standards of goods and services. Transparent and traceable ownership histories would reveal any historical fraud, theft, use of forced labour, links to violence, drugs or arms trafficking or other dubious practices, improving the capacity to enforce the law and enabling more responsible consumption. However, there are reasons to be cautious. Trust between participants depends on trust in blockchain technology, but this is not completely free from vulnerabilities, including both accidental errors and malicious attacks. Automation will not guarantee the elimination of bugs, conflicts of interest or corruption in complex global supply chains.

Blockchain offers pseudonymity; in other words, all transactions are transparent, but they are not explicitly connected to real-world individuals or organisations, shielding the identity of parties along the supply chain without compromising the integrity of the record. Checking attributes of goods and their movements can be decoupled from the full identity of the users, concealing sensitive detailed personal data beyond what is required for the record. However, this anonymity is not absolute and, with enough effort, it can be possible to connect transactions to particular parties. While this is, broadly considered an improvement on the current system, there may be implications for privacy. Once the goods reach the consumer, detailed tracking should cease or, at least, comply with privacy and data protection standards.

Anticipatory policymaking

Blockchain development in supply chain management presents significant regulatory challenges. Regulations such as the European directive on non-financial reporting could have an impact on blockchain applications for supply chains. This requires companies to disclose reliable information about environmental matters, social and employee aspects, respect for human rights, and anticorruption issues, thus pushing for more transparency in their operations. However, the absence of an intermediary in most or all steps of the supply chain in the future could create uncertainty for the parties involved, especially when it comes to automatised forms of execution and supervision of transactions. In most cases, notions and mechanisms for liability and responsibility when unforeseen problems occur need to be in place, but also potentially to be reworked.

7 Blockchain states: rethinking public services

In the context of opening up data, services and decisions in the public sector through digital technologies, a new generation of open, accountable, transparent and collaborative eGovernment services are under development. The UK Government Chief Scientific Advisor recently published a report outlining how blockchain-based technologies could provide new tools to reduce fraud, avoid errors, cut operational costs, boost productivity, support compliance and force accountability in many public services. Potential applications include tax collection, identity management, distribution of benefits, local (or national) digital currencies, property and land registry and any kind of government record. The same technology also opens doors to non-state actors to provide state-like services, from notary services to global citizenship and identity. What blockchain will mean for the public sector remains to be seen.

How blockchain technology could support public services

Data used by public institutions is often internally fragmented and opaque to other actors, notably citizens, businesses and watchdogs. Blockchain technology could allow records to be created and verified with a greater level of speed, security and transparency. The most immediate applications of blockchain technology in public administrations are in record keeping. The combination of time-stamping with digital signatures on an accessible ledger is expected to deliver benefits for all users, enabling them to conduct transactions and create records (e.g. for land registries, birth certificates and business licences) with less dependence upon lawyers, notaries, government officials and other third parties.

The Estonian government has experimented with blockchain implementations enabling citizens to use their ID cards to order medical prescriptions, vote, bank, apply for benefits, register their businesses, pay taxes and access approximately 3 000 other digital services. The approach also enables civil servants to encrypt documents, review and approve permits, contracts and applications and submit information requests to other services. This is an example of a permissioned blockchain, where some access is restricted in order to secure data and protect users' privacy. Similarly, the role of the state as the authority retaining control over the system contrasts with the bottom up structure of many initiatives promoted by the blockchain development community. Nonetheless, as the system is rolled out to public notaries and patient records, it remains one of the most advanced government initiatives using blockchain.

Several countries including Ghana, Kenya and Nigeria have begun to use blockchains to manage land registries. Their aim is to create a clear and trustworthy record of ownership, in response to problems with registration, corruption and poor levels of public access to records. Sweden is also conducting tests to put real estate transactions on blockchain, in this case to allow all parties (banks, government, brokers, buyers and sellers) to track the progress of the transaction deal in all its stages and to guarantee the authenticity and transparency of the process while making considerable time and cost savings.

The Department for Work and Pensions in the UK have also trialled the use of blockchain technology for welfare payments. Here, citizens use their phones to receive and spend their benefit payments and, with their consent, their transactions are recorded on a distributed ledger. The aim of the initiative is to help people manage their finances and create a more secure and efficient welfare system, preventing fraud and enhancing trust between claimants and the government. The UK government is also considering how blockchain technology could enable citizens to track the allocation and spending of funds from the government, donors or aid organisations to the actual recipients, in the form of grants, loans and scholarships.

Potential impacts and developments

Introducing blockchain technology to public administrations could lead to streamlined internal processes, reduced transaction costs, more trusted interactions and data exchanges with other organisations and governmental silos, and increased protection against errors and forgery. Some processes could also be automated via smart contracts. However, there are also risks that must be considered. First, in moving to a new system for digital records, there will be set-up costs and potential technical and procedural difficulties in running back-up and parallel systems during transitional phases. Furthermore, it is important that expectations for the custody and control of public records at the time the records were created continue to be respected long after they are created. Finally, since the technology stores hashes (described in the patent section) or other incomplete digital representations of documents, private individuals and organisations will need to invest further resources to preserve their documents in the long term.

While blockchain ledgers can record the time and details of a transaction, they cannot verify the accuracy of what is described within it. As long as the transaction complies with the technical requirements of the protocol, it will become an immutable part of the record, regardless of the veracity of its content. Just as all information requests and submissions to public offices are scrutinised before being implemented, it remains necessary to ensure adequate controls for accepting and sharing information on their blockchain equivalents. While it may, someday, be possible to automate, support and secure some of these processes, they are not considered a replacement for the gate-keeping role of civil servants.

The fact that data in the blockchain is immutable – which means that it cannot be altered or removed once it has been entered – provides transparency and accountability. However, it may also compromise privacy and data protection, especially when it comes to personal or sensitive data (which should never be stored on a blockchain). Blockchains do not guarantee anonymity and, the more personal the data is, the easier it is to identify the individual to which it pertains. This immutability may compromise the 'right to be forgotten', whereby users may, under certain circumstances, demand that their personal data be erased.

It is important to ensure that all citizens are able to access their public services. There is a risk that blockchain could exacerbate the existing digital divide. Citizens who are unable to use internet services for whatever reason may not be able to take full and direct advantage of the blockchain developments that would give them more control over their data and transactions. Often, the blockchain-based services would be hidden beneath familiar and user-friendly service interfaces. The precise implementation of the protocol in terms of both its structure and its user interface matters a great deal to the political and social values promoted by the system. Finally, it is worth noting that some blockchain initiatives promote the circumvention of traditional, centralised institutions and authorities, including governments and public services. Blockchain-based 'state-like' services offered by non-state actors are already emerging. These may appeal to increasingly digitised and globalised communities but could also present complex challenges for state authorities.

Anticipatory policy-making

Public administrations are likely to retain substantial central control over their blockchain implementations, and may also demand 'backdoors' to private encrypted blockchain systems for law enforcement purposes, although these may introduce new security vulnerabilities. End-to-end encryption may also be considered in the upcoming review of the EU's ePrivacy Directive. Governments may consider how blockchain might help them improve public services, particularly in providing transparency and accountability, and whether they should recognise independent 'state-like' services within their jurisdictions.

8 Blockchain everything? Decentralised autonomous organisations

Early internet pioneers envisioned a new social order of more independent, decentralised and agile organisations facilitated by information and communication technologies. Some argue that peer-to-peer and commons models would manage resource use better, and others are already developing platform cooperatives that are collectively owned and democratically governed by their users or workers. Blockchain can support such organisations by allowing for the direct and instantaneous exchange of data or property, execution of budgets, automatic enforcement of contracts or decision-making inside an organisation, all in a transparent and encrypted form. Could this herald the emergence of new blockchain-enabled organisations, and what would this mean for European society?

Decentralised ledgers for decentralised organisations

Decentralised autonomous organisations (DAOs) can be understood as bundles of smart contracts, culminating in a set of governance rules that are automatically enforced and executed through blockchains. A DAO could adopt a mediating role between different parties in a decentralised but ultimately human-controlled organisation, or it might constitute a more fully autonomous organisation that is controlled entirely through algorithms. The level of autonomy and self-sufficiency that DAOs will reach remains to be seen. The most mature DAO – named 'The DAO' – is not fully autonomous, although a future in which other DAOs are almost completely independent of human intervention, controlling their own resources and interacting with other humans and non-humans, including other DAOs, is not beyond imagining. For example, a DAO could own a self-driving car that acts as a taxi 24 hours a day. This would generates income that it would use to pay for its own fuel, repairs and insurance, and save money to replace the vehicle at the end of its useful life.

In DAOs, cooperation between people within and between organisations can be based not on centralised authority or pure market forces but, instead, on cryptographic consensus and transparency as basic technical features. Smart contracts on the blockchain have the potential not only to leave a tamper-proof record of every aspect of an organisation, but to automatically and even autonomously execute daily operations, such as supporting access to assets and buildings, allocating tasks, managing shares and voting rights, or facilitating profit distribution or transmission of micropayments.

It has been suggested that blockchain technology could enable a new generation of organisations to change the economic and power dynamics of traditional centralised bodies. For example, a social media platform owned by its users who rate each other and are automatically rewarded for their contributions; ride-sharing apps where drivers also co-own and manage the daily operations, or other communities such as Steem-it where users are also shareholders and where value and decision-making are distributed in a transparent way.

Potential impacts and developments

Blockchain can be used to develop decentralised structures inside organisations. But at the same time, using blockchain for every transaction could limit flows of information that were, until now, predominantly free. Supervising and controlling access to every transfer of any asset or content could lead to stronger intellectual property claims (for instance in digital rights management), and could stifle innovation and the rise of new players. By removing centralised management, DAOs could eliminate the errors and corruption introduced by humans. Trust will shift from traditional reputation to techno-social networks (as in blockchain-enabled contracts and

currencies). Some argue that this could bring about new forms of democratic collective action, transforming top-down governance approaches that are criticised for their inflexibility, opacity, slowness and democratic deficit.

The DAO raised over €100 million in the largest crowdfunding campaign ever. It is a mix between a crowdfunding site and a venture capital fund based on Ethereum smart contracts. Funders vote to decide everything from nominating and firing its curators to financing projects. In June 2016 an attack exploited weaknesses in the DAO's code, siphoning almost one third of its assets and sparking a controversy in the community about what to do next. The options were to freeze funds in the account (a 'soft fork'), to hack the system and restore the original balance (a 'hard fork'), or to do nothing at all. On one hand, since the attacker(s) exploited a weakness in the code, it could be argued that they did not breach the contract and that modifying The DAO's blockchain would undermine public confidence in its principle of immutability. On the other hand, the attack clearly went against the spirit of the contract, may have contravened contract law and could discourage actual and potential participants in the community. In any case, the incident exposed existing security vulnerabilities and tested the ideological foundations of the blockchain development community.

Resistance to using existing legal structures (for example treating core developers and miners as fiduciaries) led to calls for more sophisticated or alternative mechanisms, such as reputation/meritocratic systems to incentivise participation, or for the adoption of shared norms and ethical standards. However, the autonomous workings of such organisations also raise concerns over delegation to and regulation by algorithms. Some argue that such distributed governance by code still implies moral duties or responsibility on the part of the community to intervene in crucial decisions, while others are working towards embedding human values and the general will of citizens into algorithmic social contracts.

Anticipatory policymaking

DAOs, like many blockchain-based initiatives, exist in a regulatory grey zone that may not offer liability, protection or accountability guarantees, particularly when they are not explicitly grounded in existing legal systems. There is also legal concern over equity offerings in crypto companies, which may place companies within the existing securities market requiring registration and conformity with a number of rules and obligations. By operating outside of a regulatory framework, blockchain-based organisations that are not incorporated or legally recognised may be at risk of investment fraud and malicious hacks, and their members could be exposed to liabilities as partners. Some have called for greater oversight and transparency in algorithmic decision-making and interactive modelling. The complexity of advanced algorithms makes it difficult even for developers to fully understand their governing rules, and to check their legal compliance, for example with anti-discrimination and transparency laws. Self-running and self-enforcing organisations could also challenge traditional notions of legal personality, individual agency and responsibility.

DAOs could be programmed to trade in illicit goods or banned products. Even where anonymity is not guaranteed, the efficient, automatic and distributed structure of the underlying blockchain could make it difficult for regulatory bodies to enforce the law and shut operations down. Victims of crime at the hands of a DAO may also find it difficult to recover damages, or to obtain an injunction against the malicious DAO, where the capacity to engage such measures is not specifically encoded within its structure.

Conclusions

While blockchain's best-known, most used and highest-impact application is Bitcoin, the potential impact of the technology is much greater and wider than virtual currencies. Indeed, since other applications can 'piggyback' the Bitcoin blockchain, the biggest impacts of Bitcoin may be found outside the currency domain. Transactions of any kind are usually faster and cheaper for the user when completed via a blockchain, and they also benefit from the protocol's security. Whereas transactions in Europe are often fast, cheap and secure enough for most purposes, users and proponents of blockchain applications often see additional benefits in its transparency and immutability. Indeed, there is a growing trend towards less trust in financial and governance institutions and greater social expectations of accountability and responsibility. The popularity of blockchain technology may also reflect an emerging social trend to prioritise transparency over anonymity.

Of course, for each transaction that uses a distributed ledger instead of a traditional centralised system, the intermediaries and mediators are displaced, missing out on their usual source of power and income. For currencies these are the banks, for patents the patent office, for elections the electoral commissions, for smart contracts the executors, and for public services the state authorities. A significant level of growth in the use of blockchain technology, could see substantial change in the substance and, perhaps, quantity of 'white collar' work. For example, some of the work of intermediaries and contract lawyers could be replaced by peer-to-peer transactions and smart contracts. Many commentators are relaxed about this prospect. Some argue that only some of the less interesting tasks – such as providing proof of certification – would be displaced by blockchain, leaving more time for the core and high-value tasks of providing bespoke services. While this may still lead to some reduction in the total quantity of work, others commentators cite similarities with previous waves of automation in blue-collar work – such as robotic production lines – where repetitive tasks were displaced leading to job losses, but new high-quality jobs were created in the design and maintenance of the necessary systems. In any case, while evidence remains scarce, most commentators expect a change in the profile of tasks performed by humans with no overall reduction in the total number of jobs and, perhaps, an increase in their quality. Another potential indirect impact of blockchain development could be increased energy consumption. In 2014 the Bitcoin blockchain was responsible for electricity consumption comparable to that of Ireland, and has only grown since. While more efficient algorithms and hardware could be developed, the energy intensity of blockchains (and, indeed, that of all digital processes) may become an increasing problem in the future.

The most profound effect of blockchain development could be found in more subtle impacts upon broad social values and structures. These impacts are associated with the values that are embedded within the technology. All technologies have values and politics, usually representing the interests of their creators. In this light, the reasons why traditional ledger systems position their creators as the central intermediaries are clear: since all transactions pass through them, the creators maintain their position of power and capacity to profit from their users. In using technologies, people reaffirm the values and politics that they represent, so each time these ledgers are used to record a transaction, the centrality and indispensability of the actor at its centre is reaffirmed. Of course, a distributed ledger without a central intermediary is also value-laden and political, placing trust in encryption and networking technology and redistributing power from central authorities to non-hierarchical and peer-to-peer structures. In this context, to use this kind of blockchain *is* to participate in a wider shift that would reduce the trust in and power of traditional institutions, such as banks and governments. The cases explored in this report reveal several examples of how blockchain applications embody these values. Of course, for these changes to be noticeable on a general social level would require really substantial development of blockchain to the point where it permeates daily lives and mundane routines.

Anticipatory policymaking

At first glance, the decentralised, encrypted and self-executing character of blockchain technological applications does seem to rely upon or assume a self-regulatory approach that would in principle operate in parallel to the traditional legal instruments. However, looking more carefully at the most advanced blockchain applications, a mixture of traditional and novel legal and regulatory questions are raised that must be considered in a contextual manner as some of the above-mentioned applications challenge fundamental tenets of law and diffuse the object of regulatory attention, as such, in a variety of ways.

First of all, the decentralised, cross-boundary character of blockchain raises jurisdictional issues as it seems to diffuse institutional accountability and legal responsibility in an unprecedented manner, rendering the need for a harmonised regulatory approach at the transnational level more pertinent compared with a local or regional one. If blockchain technology developed significantly, centralised structures of law might lose their ability to control the ledger, with control passing to their users or other parties in the system, or to shape the activities of disparate people or autonomous decentralised organisations, as no one (including the original creator) can control the ledger after it has been deployed. There will be fewer checkpoints to guide and assist the flow of data. There are also various issues that need to be considered such as the legal enforceability of smart contracts, and liability and accountability issues, as distributed ledgers currently lack the legal personality that is necessary for them to be assigned with responsibilities and liabilities. This issue is exacerbated by the fact that they operate across borders and that smart contracts may not yet be capable of performing complex operations.

Decentralised blockchain-based systems may be open to co-option by external powers and, in the absence of sufficient institutional protection, the platforms could evolve into oligarchies. An ill-intentioned decentralised autonomous organisation could be a source of regulatory concern in view of the potential for this transformative technology to be misused. Moreover, the encrypted qualities of blockchain technology may eliminate the possibility for legitimate forms of surveillance used for prosecution and law enforcement. Consumer protection will also be a key concern of regulators, as the contractual clauses and redress measures may not be clear to consumers and, given their automated character, not easily adjustable to a possible change of circumstances. Furthermore, there are security concerns of a regulatory nature, as it could be possible to trace or deduce a party's identity from transactions. Finally, blockchain may lead to questions about the choice of law and jurisdiction for the adjudication of the relevant disputes.

It is worth noting that interest in blockchain-based applications often appears to be wedded to discontent with traditional systems, processes and mediators. Blockchain development often exhibits similarities with the sharing economy in the sense that they promise to connect individuals with others, ousting middlemen and unburdening people from the intervention of states, banks and other grand institutions, often with a rhetoric of transition, disruption or even revolution. However, as has been seen, the most successful initiatives of this movement have become the ultimate middlemen, structurally very distant from the vision of decentralisation that many citizens expected. The same may be seen with blockchain, with the greatest impact occurring in applications that appear distant from the more idealistic vision of blockchain development as decentralised and transparent. For example, an electoral authority could implement a permissioned blockchain-based voting system, maintaining control over the distribution of pseudonyms to guarantee anonymity and affirming their role as the ultimate

authority and central mediator through which all votes must pass. This is not to deny the potential technical and political advantages of such an approach. Rather, it is a reminder that, in this kind of permissioned blockchain, the level of decentralisation and transparency are all reduced, with consequences for the technical structure and functionality of the ledger, as well as for the values and politics that it reflects. It is possible to imagine several parallels for land registries, banks and patent offices, each of which could adapt technical aspects of the blockchain protocol, while moderating the idealistic elements of the values that are embedded within it. These systems would still likely offer substantial improvements in terms of increased transparency and accountability, and reduced corruption. Indeed, by co-opting blockchain, governance institutions could use it to create 'regulatory technologies' that are deployed to achieve the same regulatory objectives – e.g. transparency or accountability – as existing laws.

Since middlemen are displaced by the blockchain, such intermediaries cannot be relied upon to regulate their operation. As such, alternative regulatory levers must be developed to uphold the law and maintain the capacity for effective planning and action. Four broad categories of action that governance institutions could mobilise in response to the emergence of blockchain technology can be identified:

- One option is to respond to 'the problems to which blockchain is a solution' without using blockchain at all. For example, if demand for blockchain is based upon a desire for more transparency in processes, then citizens could be granted more access to government data and processes without using blockchain systems at all.
- A second option is to actively encourage development and innovation of blockchain by the private sector by granting legitimacy to their products. For example, under some conditions, transactions on blockchains could be given explicit legal recognition as records of executed transactions.
- A third option is to do the reverse of the previous one, i.e. discourage development by refusing to accept the legitimacy of blockchain-based transactions, for example by overruling and reversing the clauses in smart contracts.
- A fourth option is to adopt a permissioned blockchain in existing systems and structures, effectively maintaining the role and power of those responsible as middleman by providing some of the basic functionality of blockchains, but without offering full decentralisation and transparency. This model is already observed in public sector use of blockchain technology, for example in the UK and Estonia, as well as in the private sector.

Variations and combinations of all four strategies are likely to be applied to blockchain technology in different domains and jurisdictions over the next decade. For the moment there is little appetite for intervention at a European level. Indeed, a recent European Parliament report on virtual currencies acknowledged the increased risks, which will require enhanced regulatory capacity and adequate technical expertise, while calling for a proportionate EU regulatory approach in order not to hamper innovation at such an early stage.

To conclude, the fact that the blockchain protocol provides platforms for both good actions and bad actions does not mean that it is a neutral technology. In its purest form it promotes a redistribution of power from central actors across wide communities of peers. While the most idealistic and revolutionary visions of blockchain development will probably remain no more than visions, even moderate implementation of blockchain may still promote some degree of redistribution and transparency. As Glyptis notes, blockchain will not make better people, but it might make some of the precautions necessary in people's daily lives faster, cheaper, more secure and more transparent.

Blockchain technology is of increasing interest to citizens, businesses and legislators across the European Union. This report is aimed at providing a point of entry for those curious about blockchain technology, so as to stimulate interest and provoke discussion around its potential impact. A general introduction is followed by a closer look at eight areas in which blockchain has been described as having a substantial potential impact. For each of these, an explanation is given of how the technology could be developed in that particular area, the possible impacts this development might have, and what potential policy issues are to be anticipated.

This is a publication of the
Directorate for Impact Assessment and European Added Value
Directorate-General for Parliamentary Research Services, European Parliament

PE 581.948
ISBN: 978-92-846-0549-1
doi 10.2861/926645
QA-02-17-043-EN-N