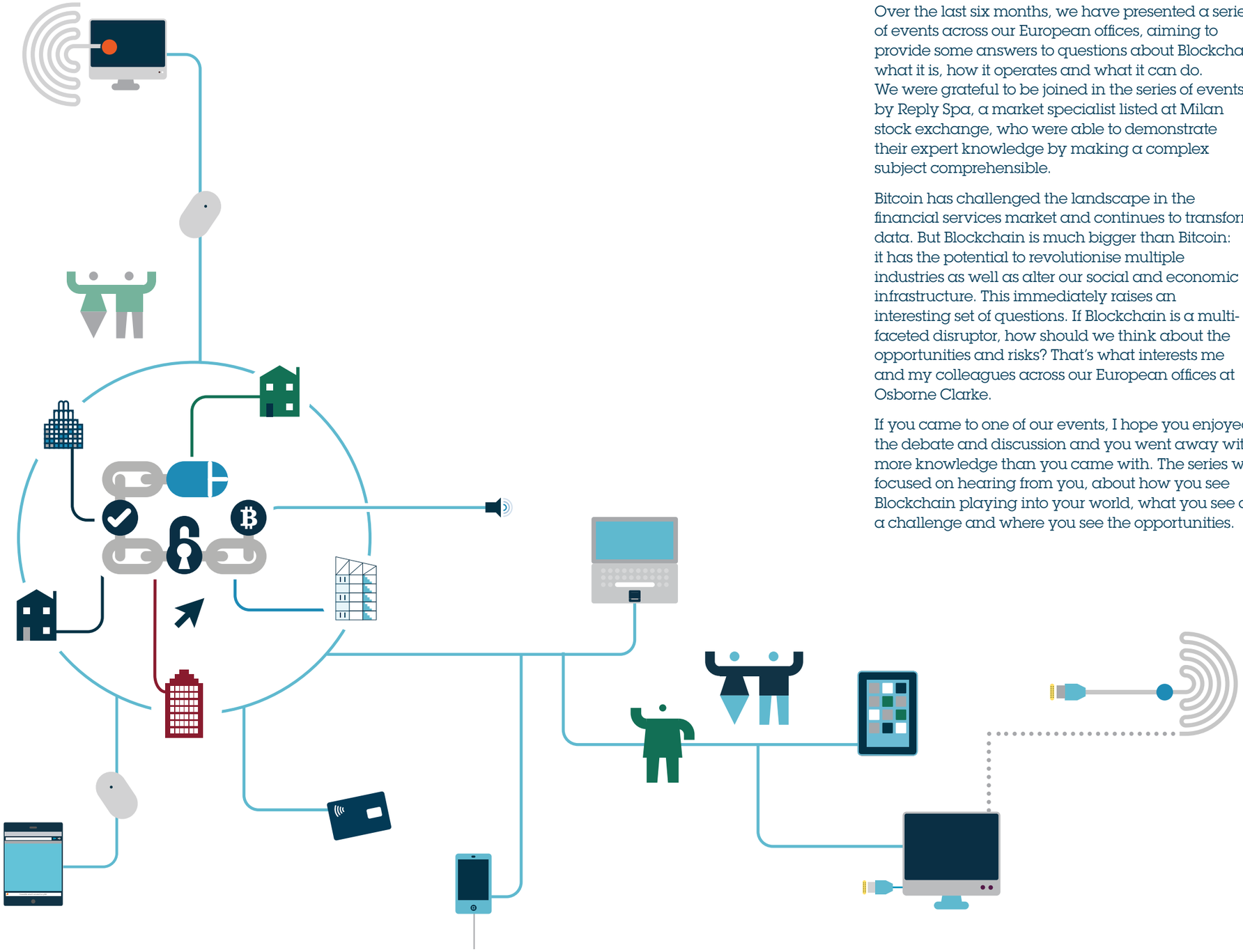
Osborne Clarke International Blockchain Report

Beyond Bitcoin: Why Blockchain matters to your business

June 2017

Start



Foreword

Over the last six months, we have presented a series of events across our European offices, aiming to provide some answers to questions about Blockchain: what it is, how it operates and what it can do.
We were grateful to be joined in the series of events by Reply Spa, a market specialist listed at Milan stock exchange, who were able to demonstrate their expert knowledge by making a complex subject comprehensible.

Bitcoin has challenged the landscape in the financial services market and continues to transform data. But Blockchain is much bigger than Bitcoin: it has the potential to revolutionise multiple industries as well as alter our social and economic infrastructure. This immediately raises an interesting set of questions. If Blockchain is a multi-faceted disruptor, how should we think about the opportunities and risks? That's what interests me and my colleagues across our European offices at Osborne Clarke.

If you came to one of our events, I hope you enjoyed the debate and discussion and you went away with more knowledge than you came with. The series was focused on hearing from you, about how you see Blockchain playing into your world, what you see as a challenge and where you see the opportunities.

As a follow up to the events, we want to provide you with some unique insights by replaying some of the questions asked at each of the events and our responses to those.

These will give you some sense of regional variations in thinking and approach across Europe and the differences in local legal regulation. In addition to these questions we have put our minds to what we think are the key legal issues impacting the use of Blockchain technology:
Data Protection, IP and Smart contracts.

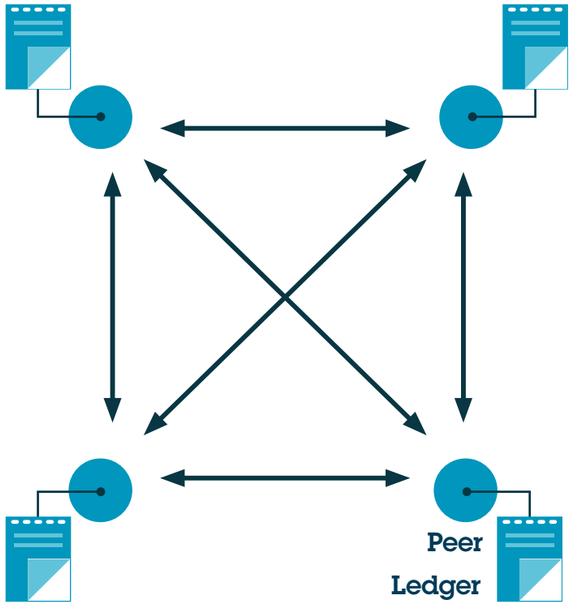
Thank you for your contribution. We hope the insights we have found will inspire you to learn more about Blockchain technology and the challenges and prospects that lie ahead for businesses.

Edoardo Tedeschi
Partner
Osborne Clarke Italy

A recap: What is Blockchain all about?

Blockchain technology was first implemented to support the cryptocurrency Bitcoin, by providing a database which could record all transactions involving Bitcoin, in a way that was secure, durable and de-centralised. It was soon realised that those attributes made Blockchain technology a powerful solution that could be used in a variety of different applications.

Blockchain technology: key features



- **Peer-to-peer network logic** widely accessible.
- **Distributed ledger** constantly updated for every network node (no single-point-of-failure).
- **Disintermediation of any Trusted Third Party** via a censorship-resistant model.
- **Open source** software, often open source (to allow for independent checking of the code) and maintained by a community of developers.

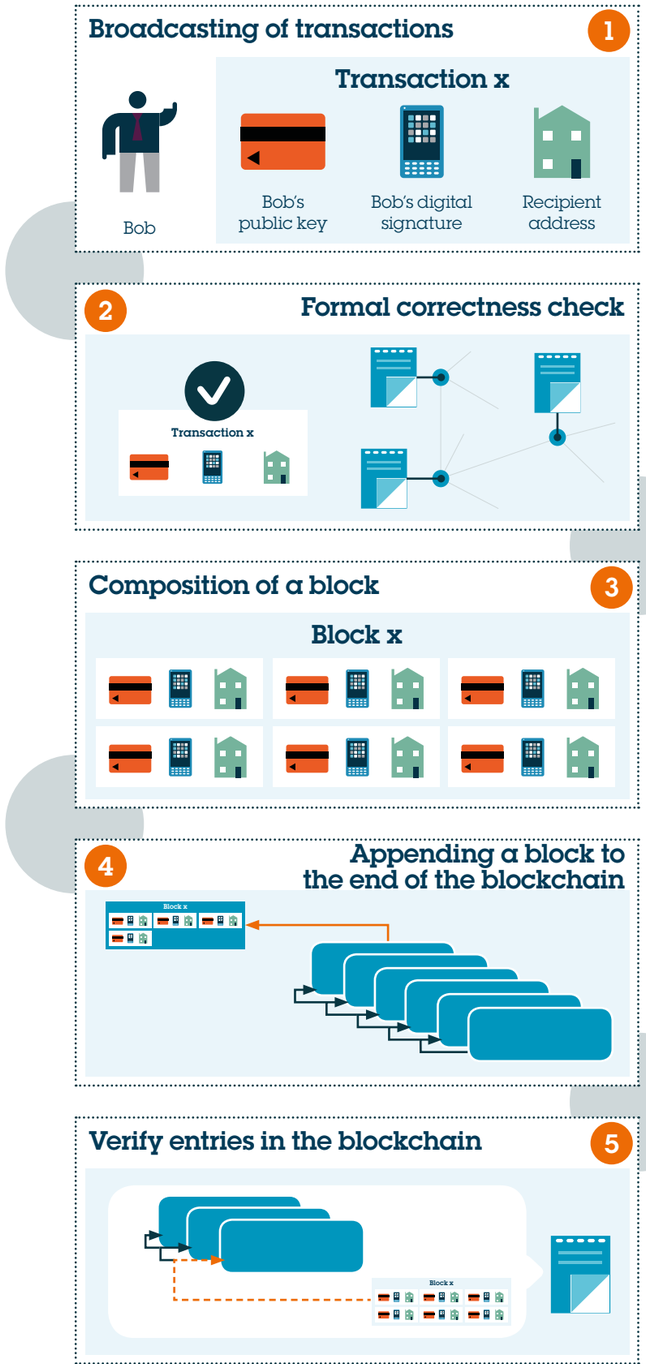
At our Paris event, we were asked about the nature of the relationships between the different stakeholders involved in a particular Blockchain application.

As is often the way in commercial transactions, the key is to define the contractual model clearly.

- In a **private Blockchain** – where access to the Blockchain is controlled – this is more straightforward. The governance model can be pre-defined and participants will need to agree to the contractual model, which can allocate roles and risks between all those involved, in order to be given access.
- In a **public Blockchain** – where anyone can view and participate – the position is more challenging. Terms of use can still be communicated to users, but may be more difficult to enforce.

The situation becomes even more complex when Blockchain technology is used to establish a **'decentralised autonomous organisation'** (DAO), which is an entity built on a Blockchain that operates independently of any central authority or service provider. For example, in April 2016, an organisation called "The DAO" was launched and attracted more than $100m in funding. However, when a security flaw in the DAO's code led to $50m of that being misappropriated, those affected were left without any viable remedy.

Anatomy of a transaction



Ledger updates occur as a multi-step process:

1. Each user broadcasts an electronically signed transaction to other peers.
2. Nodes check transaction correctness, and propagate valid ones.
3. Mining nodes collect valid messages inside a new block and keep on computing block hashes until they find a solution.
4. Once a miner finds a solving hash and wins the mining contest, it appends the new block to the blockchain ledger and broadcasts this updated version to all other peers.
5. Eventually, all peers are able to verify the status of confirmed transactions just by reading the ledger.

Smart contracts

While Blockchain technology is based on distributed ledgers, much of the interest in the technology depends not just on using ledgers for reference or provenance, but for executing actions dynamically, in the form of 'smart contracts'.

There is no universally established and accepted definition of a smart contract, but in essence it is a set of coded instructions that self-perform when certain criteria are met. Like a traditional contract, a smart contract will contain a set of rules and consequences. But unlike a traditional contract, those rules and consequences can be automated according to pre-set input criteria, functioning without further input by either party. Those actions cannot be completed unless they are validated by the other participants in the network.

Example – future trades: Smart contract allows assets and funds to be transferred automatically on the occurrence of a pre-set event (or date), with the price determined automatically according to a pre-agreed formula.

With the exception of certain types of agreement that require specific formalities (such as for the agreement to be in the form of a "deed", or to be notarised, for example), a smart contract could function as a standalone commercial agreement, if all of the necessary elements can be coded. However, more commonly (at least to start with), smart contracts will have a 'traditional' contract sitting alongside them, to address any issues that cannot be captured in the smart contract code. That would include more subjective or difficult-to-define provisions, along with terms such as the applicable law and jurisdiction, and how any disputes should be resolved.

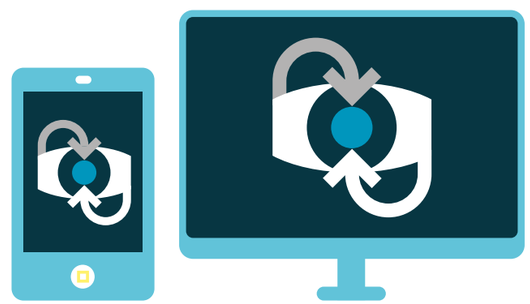
At our Madrid event, we were asked about the validity of the formation and execution of smart contracts, this raised a number of issues:

Consent: as in many other jurisdictions, one of the key elements required for a valid contract is consent (or acceptance). The Spanish Civil Code recognises a wide range of forms of giving consent, and a single consent can be given for multiple transactions. However, valid consent requires the person giving consent to be informed and conscious of the rights and obligations set out in the contract. The current legal framework may need to be revised if it is to capture more complex uses of smart contracts, such as DAOs, which in the absence of any directing natural or legal person would be unlikely to be considered to have capacity to give consent and enter into a contract.

Formation and execution: smart contracts will be formed and executed electronically. In the EU, this will usually be sufficient to be legally enforceable, as the EU has a framework for the recognition of electronic signatures. This distinguishes between different types of electronic signature, but preserves the legal admissibility of each type. However, individual jurisdictions may require additional formalities, such as notarisation, for certain types of contract, so there may be certain types of transaction for which smart contracts would not currently be valid under existing legal rules.

Location: being electronic and de-centralised, parties and participants in a Blockchain can be distributed across the globe. This could create difficulties, since different jurisdictions will have different provisions as to where a transaction is considered to have taken place. It can help to designate upfront where any transaction is deemed to have taken place, and which jurisdiction and choice of law the parties are electing shall apply, but there may be jurisdictions or types of agreement or legal issues for which such self-determination is not recognised.

Timing of transactions: different jurisdictions will have different provisions for the time and date on which a transaction is deemed to have taken place, which may be important in the event of a dispute. In some countries, such as Italy, time-stamping by a certified body is recognised by law. Blockchain providers may be recognised as such bodies, since an essential feature of Blockchain technology is that each transaction (or 'block') is recorded with an immutable time stamp.



Data protection

Data protection regulations are becoming increasingly stringent and pose a particular challenge for Blockchain applications, in which information is held as immutable records on a distributed global network.

One obvious question is which jurisdiction's data protection laws will apply? The answer might be more than one: the incoming EU General Data Protection Regulation (GDPR), for example, has extraterritorial reach in certain circumstances, so may apply alongside other national regulations. This could mean organisations have to comply with multiple sets of data protection rules.

At our Madrid event, we were asked who would be considered the 'data controller' and the 'data processor' for the purposes of those regulations.

The Blockchain service provider or operator would almost certainly be considered a data controller. Since data is being held and transferred by all of the other participants in the Blockchain network, they may be considered data processors or data controllers, depending on the precise set-up of the relevant Blockchain.

To allow for this, any contracts between the Blockchain service provider and the participants in the network should include appropriate provisions relating to data protection and security.

At our London event, we discussed the challenges of Blockchain involving cross-border data transfers.

The GDPR and current national laws across the EU preclude the transfer of data outside the EU without adequate protection. Protection will be considered adequate where the non-EU country has been deemed to have an 'adequate' data protection regime in place, where the organisation receiving the data is covered by an arrangement such as the EU-US 'Privacy Shield', or where bespoke contractual protections are put in place, such as the EU's 'Model Clauses'.

Turning the issue on its head, Blockchain technology could be used as a solution for maintaining data protection. The GDPR encourages concepts such as encryption and pseudonymisation, which are fundamental in Blockchain technology. However, it will take some time for regulation to catch up with technology in recognising the role that Blockchain could play here.

Right to be forgotten

A particularly challenging data protection scenario would be where a data subject requests that their data be removed – the so-called "right to be forgotten". Since one of the fundamental aspects of Blockchain is the immutability of the entries on its ledger, this could prove a technical and regulatory challenge. However, as with international data transfers, there are a number of derogations from the 'right to be forgotten'. For example, data does not need to be erased where it is required:

- to achieve the purposes for which it was originally collected; or
- to comply with a legal obligation or regulatory requirement.

This might apply, for example, to a Blockchain application that is designed to demonstrate the provenance of certain products (one current example being diamonds). In this case, the Blockchain service provider may well argue that personal data is required to be retained permanently to achieve the purpose for which it was collected.

Where there is a chance that personal data will need to be erased, one option Blockchain service providers could consider is 'tokenisation'. This involves replacing the data in the 'blocks' with unique identifiers that securely link to "tokens" holding the personal data. By doing so, operators enable the removal of the personal data where required, without compromising the integrity of the records on the Blockchain.

Public or private Blockchain?

The right approach to data protection and security will also depend on the type and purpose of the Blockchain. Access to and policing of private Blockchains is far more straightforward than for public Blockchains, where access is not controlled and the identities of participants are not always known.

Blockchains and disputes

Blockchains, by definition, will be 'distributed' – often across the globe – with participants fulfilling different functions, such as:

- the 'originator' of the Blockchain technology;
- the Blockchain service provider or operator (if different from the originator);
- the transacting parties, involved in individual 'blocks';
- miners, who verify transactions; and
- 'peer' participants in the network.

The different functions will attract different rights and obligations. Where a dispute arises – for example a fraudulent transaction – there may be a disagreement as to whether, for example, the fraud was possible due to a weakness in the underlying technology, a weakness (technical or human) in the verification of one of the links in the network, or is attributable to those involved in the particular transaction.

Enforcing smart contracts

A consideration that goes along with jurisdiction is enforceability. At our Brussels event, we were asked how the enforceability of smart contracts could be ensured.

The underlying 'traditional' contract will of course be key. However, even where the legal rights are clear, enforcing those rights becomes more difficult when parties are based in harder to reach jurisdictions. One option could be to provide that any dispute is subject to arbitration, rather than litigation, since arbitral awards can be easier to enforce in some parts of the world where enforcing foreign court judgments can be highly problematic.

Arbitration through one of the major international institutions can be prohibitively expensive for smaller transactions though. Instead, Blockchain contracts may be well suited to having disputes resolved through alternative mechanisms, designed specifically for Blockchain.

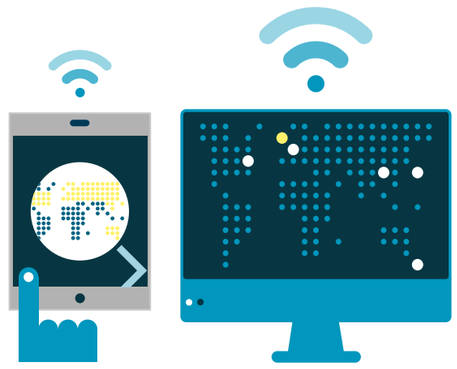
This could involve appointing an appropriately qualified arbiter, who could resolve disputes online, and who may even have some kind of digital key or form of security to aid enforcement.

It will be essential that obligations and liabilities (and any limits to those liabilities) are properly set out in contracts between the different parties (most likely through 'traditional' contracts, whether in conjunction with smart contracts or otherwise).

Contracts can also assist with another key question: which legal regime (applicable law and jurisdiction) will govern the parties' obligations, and any dispute that arises between them?

In areas like the EU, the law recognises the right for parties to choose the applicable law and jurisdiction that apply to their contract (subject to some exceptions). Where non-EU parties are involved, however, the position may not be so straightforward, and the courts of different jurisdictions may reach conflicting decisions about applicable law or jurisdiction.

The resolution of high-value, complex disputes will inevitably raise challenging issues. But having participants sign up to a first-stage online dispute mechanism – whether through specific contracts or terms of use – could help to resolve the majority of day-to-day disputes.



Blockchain in action: managing IP rights

At our Milan event, we were asked whether Blockchain technology could be used to manage rights and royalties in digital content, such as music.

This is one potential use that is generating a lot of interest in the industry. Rights to royalties can be spread among several contributors to a work, and the management of rights and royalties can be slow and far from straightforward. Blockchain, being a public and incorruptible register, can generate a certification of authenticity which is reliable, transparent and perpetual. As such, Blockchain technology could be used as a basis for systems that:

- identify the owner(s) of a work and their moral rights;
- allow the identification of authentic products, as a way of combatting counterfeitting; and
- allow revenues to be divided between holders of IP and contractual rights, automatically through a smart contract and hence more speedily.

Such applications could benefit IP rights owners in three ways:

- by helping to prevent infringement of their rights;
- by enabling them to prove the authenticity of their works; and
- by facilitating the licensing and distribution of revenues for the use of their works.

An early example of this working in action is a start-up that aims to allow artists to distribute their music directly, with consumers able to purchase licenses to stream, download or even remix songs. The Blockchain technology automatically allocates payments to the owners of the IP, and allows for payments via cryptocurrencies such as Bitcoin.

IP management societies are also showing interest, with three of the largest music collection societies (PRS, ASCAP and SACEM) in April 2017 announcing a collaboration to prototype a Blockchain-based licensing solution. But equally, blockchain solutions can fill a gap where there is currently no central authority administering those rights.

IP infringement and liability

The efficacy of Blockchain platforms as a way of managing IP rights will depend on the ability to ensure that works lodged on the platform are truly authentic. We were asked about this at a number of our events. At our Milan event, for example, we were asked whether the Blockchain service provider would be liable for any infringing content.

Blockchain service providers would certainly need to take steps to mitigate any liability they might have if works were subsequently found not to be authentic. Their potential liability would be reduced if they were able to establish that they were an internet service provider (ISP), in which case they would not be under any general obligation to monitor the information transmitted or stored on their networks, but may be required to take down infringing content.

At our London event, we were asked what could be done to force operators of a Blockchain platform to take down illegal content.

There are tried and tested legal mechanisms for forcing platforms to take down illegal content or, failing that, having ISPs block access to offending websites. In many countries, these mechanisms are generally effective, although there will be jurisdictions in which ISPs tend to be less cooperative and legal remedies less readily enforceable.

The difference with Blockchain-based platforms is that the removal of offending content may be more difficult given the immutable nature of blocks within a particular chain. This may present technical issues, at least to start with, but solutions will need to be found: if not, Blockchain-based platforms risk being blocked in some of their most important markets.

Regulating Blockchain

A question that often accompanies disruptive technologies is how that technology should be regulated. At our Brussels event, we were asked whether there were any current plans to introduce a regulatory regime for Blockchain.

Like some other types of new technology, we do not see legislators attempting to regulate the technology itself. Rather, it will be specific applications of Blockchain that may be subject to regulation.

For example, there is great interest in potential uses of Blockchain in financial services, such as securities. The European Securities and Markets Authority has been looking at this and in February 2017 issued a report which looked at whether the use of Blockchain technology in the European securities market should be subject to specific regulation. The report concluded that, for now at least, existing regulation is sufficient. But the report identified issues that would need to be addressed, including in relation to identity verification and data protection. If Blockchain technology does become widely used in financial services markets, further regulation may be needed to address some of those concerns.

At our Frankfurt event, we discussed the regulation of the original Blockchain application, Bitcoin.

In Germany, cryptocurrencies like Bitcoin are not treated as either currency or electronic money, since they are not issued by a central entity and have no legal basis obliging other entities to accept or redeem them. Instead, they are treated as financial instruments (and 'accounting units' for tax purposes), meaning that activities such as offering cryptocurrencies for sale or running sale or exchange platforms are regulated activities.

When Bitcoins are transferred, the absence of a central clearing or settlement intermediary means that there is no regulated payment service, so the Bitcoin 'miners' that verify the transaction are not subject to current anti-money laundering regulations. The same would apply for any other Blockchain-based transaction.

The challenge for legislators is identifying where existing regulation is not adequate to deal with the novel challenges posed by Blockchain, without stymying the development of Blockchain applications that can bring great benefits to consumers and industry. There will not be one catch-all solution; individual regulators and legislators in different sectors and countries will need to decide what is needed in their area.

Identification and verification

One of the paradoxes of Blockchain technology is that for some of the legal challenges the technology faces, Blockchain could itself be a solution. This is neatly illustrated by the issue of verification. In applications such as financial services or hosting of digital content, verification of identity and authentication are key challenges. At the same time, there are a number of initiatives and start-ups looking at how Blockchain technology can be used to create secure digital IDs that could be used to access both new and traditional services that require identity verification.

At our Amsterdam event, we were asked whether Blockchain could offer the same high degree of trust currently afforded to the use of notaries.

When it comes to technical verification, this is certainly possible. Highly-distributed ledgers mean that once an individual or company has established a digital ID, this can be assigned a cryptographic key, and its use subsequently will be subject to a high level of scrutiny. However, notaries also play an important advisory and independence function, which could not easily be replicated by a Blockchain-based solution.

Blockchain may also provide a solution to real time verification for financial services. Some solutions, such as e-Certificates, do not satisfy customer due diligence requirements in the Netherlands. Other solutions can provide a reliable identity checking service for the purposes of anti-money laundering regulations, without the need for face-to-face interactions. But new solutions are needed where real time verification is needed, particularly for micro transactions where manual checks are not practicable. Blockchain-based digital IDs may provide a powerful solution.

Blockchain in action: supply chains

The provenance of component parts of a wide variety of goods, from technology to pharmaceuticals and food, can be a major issue for retailers. In addition to product safety and regulation, the origin of goods can be a reputational issue in some sectors in particular.

Blockchain technology can offer a powerful solution, enabling components to be marked with a 'water mark'. This mark could represent a code which is physically attributed to single items, which are registered on the Blockchain. The advantage of the water mark is that it allows both traders and consumers to ascertain the provenance of the marked items, which can also combat counterfeitting of those items.

For example, food and beverage provided for sale to consumers in the EU must bear a label that includes certain information, which must be accurate, clear and easily understandable to allow consumers to make informed choices and to prevent any practices that may mislead the consumer. Blockchain technology could provide the best solution to track the product from the producer to the seller and to permit the fullest control over the product, its provenance and the compliance of its labelling with all applicable regulations.

Blockchain technology could also be effective in the healthcare sector. A number of start-ups are currently working on Blockchain solutions which involve the management of medical data, medical records and payment of invoices through a Blockchain platform. Recording patients' medical history on a common system would make it easier to find and share information with doctors, hospitals and clinics and could be integrated with a pharmaceutical products recorder, in order to track the provenance of the products supplied to the patient.

Summary: Blockchain uses

Blockchain's ledger update process supports a wide range of possible functionalities:

Digital Notary

Using blockchain ledger for certifying information as it provides:

– Indisputable owner

– Certain timestamp

– Immutable and persistent records

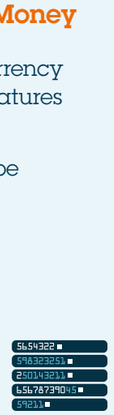
Programmable Money

Exploiting cryptocurrency programmability features in terms of:

– Expendability scope

– Authorization

– Execution time



Smart Contract

Encoding complex business rules with autonomous software agents supporting:

– Rules-based distributed computing

– Event-triggered behavior

– Interoperability with external data providers

Summary: Blockchain benefits

Blockchain applications can take advantage of a number of benefits:

Security

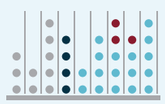
Decentralization and strong cryptography ensure immutability and persistency of information.

Interoperability

Blockchain protocols adoption facilitates sharing of common communication and security standards.

Bulletproof automation

Complex rules can be encoded on a Blockchain via smart contracts for ensuring shared and custom business logics execution.



Auditability

High accessibility and availability of information stored inside a Blockchain ledger for all network nodes.

Osborne Clarke: facts & figures

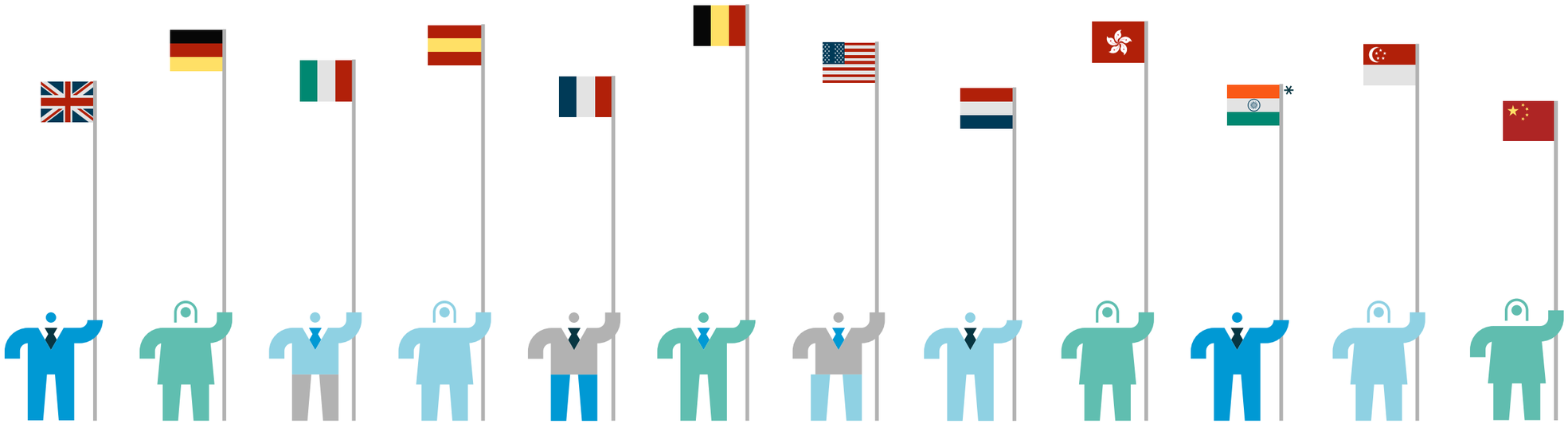
1,500

employees
and counting

12

countries

Belgium: Brussels
China: Shanghai
France: Paris
Germany: Berlin, Cologne, Hamburg, Munich
Hong Kong
India: Mumbai*
Italy: Milan, Brescia, Padua, Rome, Busto Arsizio
The Netherlands: Amsterdam
Singapore
Spain: Barcelona, Madrid, Zaragoza
UK: London, Bristol, Thames Valley
USA: San Francisco, Silicon Valley, New York



Osborne Clarke is the business name for an international legal practice and its associated businesses. Full details here: osborneclarke.com/definitions
*Relationship firm

Our Blockchain team

Milan – 25th November 2016

Edoardo Tedeschi
Partner, Italy

T: +39 02 5413 1757
edoardo.tedeschi@osborneclarke.com

Amsterdam – 30th March 2017

Jeroen Lub
Partner, The Netherlands

T: +31 207 02 8616
jeroen.lub@osborneclarke.com

London – 19th January 2017

Mark Taylor
Partner, UK

T: +44 20 7105 7640
mark.taylor@osborneclarke.com

Brussels – 27th April 2017

Benjamin Docquir
Partner, Belgium

T: +32 2 515 93 36
benjamin.docquir@osborneclarke.com

Madrid – 13th March 2017

Rafael García del Poyo
Partner, Spain

T: +34 91 576 44 76
rafael.garciadelpoyo@osborneclarke.com

Frankfurt – 4th May 2017

Matthias Terlau
Partner, Germany

T: +49 221 5108 4088
matthias.terlau@osborneclarke.com

Paris – 30th March 2017

Lise Breteau
Partner, France

T: +33 1 84 8 24552
lise.breteau@osborneclarke.com

With special thanks to Margherita, Ian and Alessandra for developing content and knowledge for this report.

Margherita Gnech
Trainee, Italy

T: + 39 02 5413 1795
margherita.gnech@osborneclarke.com

Ian McKenzie,
Senior Associate, UK

T: +44 20 7105 7558
ian.mckenzie@osborneclarke.com

Alessandra Bianchi
Senior Lawyer, Italy

T: +39 02 5413 1770
alessandra.bianchi@osborneclarke.com

June 2017
Publication number
580824