LEGAL AND REGULATORY FRAMEWORK OF BLOCKCHAINS AND SMART CONTRACTS

a thematic report prepared by

THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM

EU Blockchain Observatory and Forum

An initiative of the European Commission

About this report

The European Union Blockchain Observatory & Forum has set as one of its objectives the analysis of and reporting on a wide range of important blockchain themes, driven by the priorities of the European Commission and based on input from its Working Groups and other stakeholders. As part of this it will publish a series of thematic reports on selected blockchain-related topics. The objective of these thematic reports is to provide a concise, easily readable overview and exploration of each theme suitable for the general public. The input of a number of different stakeholders and sources is considered for each report. For this paper, these include:

- Members of the Observatory & Forum's Working Groups as well as the Obeservatory's Legal Sub-Working Group (please see next page).
- "Legal Recognition of Blockchain Registries and Smart Contracts", by Dr Robert Herian of the Open University Law School, an affiliate of the Knowledge Media Institute of the Open University, which is an academic partner of the EU Blockchain Observatory & Forum.
- Input from participants at the "Legal Recognition of Blockchains & Smart Contracts" workshop held in Paris on 12 December 2018.
- Input from the Secretariat of the EU Blockchain Observatory & Forum (which includes members of the DG CONNECT of the European Commission and members of ConsenSys).

CREDITS

This report has been produced by ConsenSys AG on behalf of the European Union Blockchain Observatory & Forum.

Written by: Tom Lyons, Ludovic Courcelas, Ken Timsit
Thematic Report Series Editor: Tom Lyons
Workshop moderator: Susan Poole
Report design: Benjamin Calméjane

v1.0 - Published on 27 September, 2019.

DISCLAIMER

ACKNOWLEDGEMENTS

The EU Observatory & Forum would like to expressly acknowledge the following for their direct contributions and feedback to this paper as members of the Legal Sub-Working Group:

- Anastasios A. Antoniou
- Cristina Carrascosa Cobos
- Tamás Chlepkó
- Marina Cugurra
- Michèle Finck
- Jānis Graubinš
- Marta Ienco
- Iwona Karasek
- Ad Kroft
- Leila Nassiri-Jamet
- Marina Niforos
- Lukas Repa
- Thomas Richter
- Philip Sandner
- Javier Sebastian
- Nina-Luisa Siedler
- Ivona Skultetyova
- David Suomalainen
- Konstantinos Votis

NOTE

While we have done our best to incorporate the comments and suggestions of our contributors where appropriate and feasible, all mistakes and omissions are the sole responsibility of the authors of this paper.

Contents

Executive summary

In this paper we examine the intersection of blockchain and the law.

Our analysis begins with **an overview of legal issues as they pertain to blockchain technology** per se, and in particular issues that arise due to the decentralised nature of many blockchain-based platforms. **We follow this with a look at the legal implications of different kinds of smart contracts.**

These include **smart legal contracts, which are smart contracts on a blockchain that represent - or that would like to represent - a legal contract** as well as **smart contracts with with legal implications, which are artefacts/constructs based on smart technology that clearly have legal implications**, for instance in the form of digital assets, or decentralised autonomous organisations (DAOs) or other kinds of autonomous agents..

These issues are, we believe, extremely important at the moment – of keen interest to the European blockchain industry as well as policy makers looking to cement Europe's position as an attractive location for this promising new technology.

If blockchain will indeed become the catalyst for innovation, jobs and economic growth in the EU that many hope, then **there is no doubt that a key element will be a predictable legal and regulatory framework for blockchains and smart contracts.**

But the new paradigms for platforms, applications, agreements and assets (among other things) enabled by blockchain are not necessarily easy to reconcile with existing legal and regulatory norms. As we try to emphasise in this paper, that does not mean such reconciliation is impossible. Quite the contrary.

First to the challenges.

The innovative aspects of blockchain are generally traceable to a few of its fundamental characteristics, namely: decentralisation, pseudonymity/anonymity, immutability and automation. These characteristics are also often at the root of difficult legal and regulatory questions raised by blockchain.

INTRODUCTION: THE NEED FOR LEGAL AND REGULATORY CLARITY FOR BLOCKCHAIN

Take decentralisation. In large-scale, decentralised blockchain-based networks – and in particular public/permissionless ones – it can be difficult to ascertain who the actors in the network are, where they are located, and what exactly their actions have been. That can make it challenging to assign responsibility or determine jurisdiction in the case of disputes. **This in turn can make it difficult to perform basic legal and regulatory functions, such as ascertain liability, determine what law is applicable in a particular situation, carry out regulatory monitoring, or enforce rules.**

In such an environment it is no wonder that many of the promising innovations in blockchain, whether digital assets, self-executing legal agreements, decentralised organisations or fully autonomous agents that act on their own, also pose legal and regulatory conundrums.

Yet none of these challenges, in our opinion, are insurmountable.

History shows that **disruptive tech and the law always find each other** in the end. We see no reason why a similar process will not enfold for blockchain. In our opinion, this will occur on two main tracks.

First will be the **evolution of legal and regulatory "tools"** to assist authorities with some of the novel aspects of blockchain technology. Many of these already exist. As is the case today with the Internet, authorities have recourse to various "access points" – exchanges for example – to help them monitor and enforce legal and regulatory requirements even in highly decentralised, permissionless environments. The blockchain industry itself has also been developing tools that can assist authorities (and blockchain companies) in enforcing regulatory compliance – for example methods to "pierce the veil" of pseudonymity on blockchains and identify network participants.

Second will be **the natural evolution of the legal and regulatory framework to take account of blockchain**. We are already seeing a great deal of activity in this regard in the area of digital assets (and will therefore be dedicating a separate paper to this subject in the near future). When it comes to more general legal issues around the technology, smart contracts and disruptive blockchain use cases, we also see a clear increase in activity by policy makers and regulators to understand the issues, to work on solutions and – importantly – to do so in conjunction with the wider community.

This latter is important. We believe strongly that if blockchain-enabled

INTRODUCTION: THE NEED FOR LEGAL AND REGULATORY CLARITY FOR BLOCKCHAIN

markets are to mature, policy makers and businesses must create the rules of engagement together. **Regulators should provide guiding principles to attract private-sector investors, ensure consumer protection and citizens' rights, and provide safeguards against anti-competitive practices.** The private sector can undertake initiatives to ensure industry-wide interoperability and compliance with existing legislation and overall public-sector objectives such as the collection of taxes and the prosecution of illicit activities.

While the overall goal is clear, the big question will be how to get there. Will existing legal and regulatory frameworks, perhaps with some clarifications and tweaks, suffice, or will we need to write new laws and rules for blockchain's new way of thinking? **We provide eight guiding principles to aid policy makers in dealing with these and other questions (detailed in the conclusion)**:

- **Craft simple yet usable definitions of the technology.** A simple but potentially quite useful first step would be for policy makers to clearly define what blockchains and smart contracts are under the law at the European level in order to have a shared definition for EU and Member State regulators.
- **Communicate legal interpretations as broadly as possible.** When blockchain is added into a law, or when a binding or highly certain interpretation of the law with regards to blockchain is reached, we think it worthwhile for authorities to make an extra effort to communicate this to the wider community.
- **Choose the right regulatory approaches for the question at hand.** When it comes to regulating new technologies like blockchain, regulators can choose from three basic approaches, each of which has its own advantages and disadvantages.
- **Harmonise the law and interpretations of it.** Whatever approach individual regulators take, we think it crucial that blockchain and smart contract regulation be as harmonised as possible throughout the EU.
- **Help policy makers develop an understanding of the technology.** Getting it right will require the respective authorities and the full ecosystem to understand this new technology and what can (and cannot) be achieved with it.
- **Work on high-impact use cases first.** In our opinion that would encompass the regulatory questions around digital assets as well as bringing clarity to blockchain and the GDPR.
- **Closely monitor developments in less mature use cases and encourage self-regulation.** As regulators know all too well,

intervening too early in novel use cases can be counterproductive.

- **Make use of blockchain as a regulatory tool.** Last but not least, we think an excellent way for regulators to help monitor and regulate the industry is to get involved themselves. For example, regulators could plug themselves into new blockchain-based platforms as they come online, unleashing new opportunities to improve the efficacy but also efficiency of their operations.

Introduction: The need for legal and regulatory clarity for blockchain

All significant new technologies, in as far as they are catalysts for change in society, will intersect at some point with the existing legal and regulatory framework.

This is certainly the case with blockchain. While its roots in Bitcoin are decidedly anti-establishment, today even mainstream proponents of blockchain and other distributed ledger technologies look at blockchain-enabled decentralisation as a way to disrupt important economic, social and political structures.

Many of these use cases exist today in a legal and regulatory limbo. This is not a priori bad nor cause for concern. Technology has always driven societal change, and the law has a long history and plenty of experience adapting to such change. At the same time, history shows us that technology must also be open to adapt to existing law where the law reflects the values and consensus of society.

In this paper we examine the intersection of blockchain and the law in Europe. Our analysis has two parts. In the first, we provide an overview of legal issues as they pertain to blockchain technology per se, and in particular issues that arise due to the decentralised nature of many blockchain-based platforms. We follow this with a look at the legal implications of smart contracts, which are an extremely important application that can be enabled by blockchains and that can be used to automate business processes and transactions as well as agreements between parties. As we will see, these characteristics can raise thorny legal questions.

Because smart contracts are the main tool used in blockchain-based platforms to create digital assets, our smart contract discussion naturally covers these as well. That said, we do so here only on a high level. As the digital asset discussion, especially with regards to the intersection of digital financial assets and existing regulation, is so vast, **we have decided**

to dedicate a separate paper to it. What we do not cover here in terms of this topic, you will find covered in detail there.[1]

CLARITY CAN SPUR INNOVATION

Achieving clarity around the questions we raise here would bring many benefits.

First, it will be important if Europe wants to cement its position as an attractive location for blockchain technology. To spur innovation, jobs and economic growth, blockchain entrepreneurs, developers, corporates and the blockchain ecosystem at large are dependent upon an easily understandable, predictable and relevant legal framework. With it, we can create the basis for a thriving new blockchain industry. Without it, startups with exciting new ideas may not pursue them for fear of future legal liability, large-scale platforms may struggle to find users as many may be wary of legal grey areas, and new types of digital assets could struggle to find buyers and sellers over concerns about running afoul of regulators.

At the same time, the EU is convinced that blockchain technology can play a key role in building Europe's Single Digital Market, and so drive important market innovations. If blockchain-enabled markets are to mature, policy makers and businesses must create the rules of engagement together. Regulators should provide guiding principles to attract private-sector investors, ensure consumer protection and citizens' rights, and provide safeguards against anti-competitive practices. The private sector can undertake initiatives to ensure industry-wide interoperability and compliance with existing legislation and overall public-sector objectives such as the collection of taxes and the prosecution of illicit activities.

While the overall goal is clear, the big question will be how to get there. Will existing legal and regulatory frameworks, perhaps with some clarifications and tweaks, suffice, or will we need to write new laws and rules for blockchain's new way of thinking?

Much of this remains to be seen. We hope our analysis can provide some food for thought to all stakeholders looking to find workable solutions.

1 Our Digital Assets paper is scheduled to appear in December, 2019. See www.eublockchainforum.eu.

Blockchain technology and the law

In this section we lay out some of the areas of tension between blockchain technology in general and prevailing legal and regulatory frameworks. Many of these tensions arise from fundamental properties of blockchain protocols, which are built on decentralised paradigms conceptually quite different from the more centralised approaches that are currently the norm.

In a typical digital platform today, a single entity stores data in the equivalent of a "master" database. This in turn becomes the single, "authoritative source of truth" on that platform, which the platform owner then shares with users. In the decentralised paradigm enabled by blockchain, a distributed, append-only database is maintained by a network of peers and acts as a "consensus version of the truth". In the old world, centrally controlled servers process information and validate data. In the new world, decentralised networks of validating nodes – often global in scope – reach consensus via a protocol and without any third-party authority.

Decentralised digital environments can be tricky from a legal perspective. They can make it difficult to ascertain who "owns" the network and its data and, therefore, who is legally responsible for it. In such a world it can be challenging to know who has processed what data, where and when, and so ascertain who is "responsible" for it, what jurisdiction applies in disputes, or who controls the information and is liable for its security or responsible for its integrity.

Blockchain-based platforms also tend to offer various degrees of pseudonymity, and in some cases anonymity, to users, making it difficult to know who is using the platform and to what end. This can make them difficult to police or regulate. Because blockchain ledgers are generally append-only and cannot be changed after the fact, they can raise issues in a number of regulatory spheres, like data privacy or consumer protection.

We look at some of the more important of these spheres of tension below. The issues discussed should not, however, be considered legal barriers to blockchain adoption, but rather as hurdles to overcome on the path towards the reconciliation of blockchain and the law.

LEGAL VALUE OF BLOCKCHAIN AS REGISTRIES

1. Blockchain and eIDAS

Blockchain was invented to facilitate decentralised, trustless transactions and, as the success of Bitcoin and other cryptocurrency platforms attests, it has so far been up to the task.

Just because we can prove mathematically that transactions on a blockchain are valid, know who "owns" the data saved in a blockchain-based ledger and demonstrate that that data has not been tampered with, does not however mean that blockchain-based transactions or registration of ownership is by itself legally

binding.

Among the prerequisites for blockchains acquiring legal status would be the legal recognition of blockchain-based signatures (who did the transaction), timestamps (when it was carried out), validations (who validated the transactions) and "documents" (that is, the data associated with a transaction or contract).

In Europe, such issues are handled under the electronic IDentification, Authentication and Trust Services regulation (eIDAS). As we have touched upon in a separate report,[1] eIDAS intersects with blockchain in different contexts.

For example, according to eIDAS digital documents cannot be denied legal force simply because they are in electronic form. This supports the potential for legal standing for the data contained in a blockchain-based registry or contract.

The situation is more complex when it comes to eSignatures and eSeals (signatures of a legal entity as opposed to a natural person). eIDAS recognises three different levels of eSignatures: simple, advanced and qualified. Blockchains would appear to meet the technical criteria for the first two.[2] But to be legally binding they need to meet the highest standard. That requires using the services of a recognised Trust Service Provider (TSP), or undergoing the arduous process of becoming a recognised TSP yourself. For this reason from an eIDAS perspective, blockchain transactions do not have legal authority by themselves.

There are related issues with timestamps. Today there is no timestamping service using blockchain that is being used by a TSP. But this can change. As authorities, including regulators and the courts, become more aware and knowledgeable about blockchain, they will be in a better position to evaluate whether blockchain-based timestamping solutions can qualify under the eIDAS framework. We believe they should be enabled and encouraged to continue to deepen their understanding in this area.

2. Recognising blockchain registries: First steps

To date, very few regulators have addressed the issue of the legal status of blockchain registries, though we can expect an increase in such activity.

That said, there has been some activity. In 2016, for instance, France recognised the use of blockchain technology as a registry in support of "minibons" through the publication of an executive order. Also known as interest-bearing notes, minibons are non-negotiable securities that contain a trader's undertaking to effect payment on a specific maturity date in return for a loan. These are mostly relevant to crowdfunding and related to non-listed SMEs.[3] And in 2017, a second executive order was published, extending the list of financial instruments that can leverage blockchain technology as a registry.[4]

These are encouraging developments from a blockchain-industry perspective. By adding a reference to blockchain to the French commercial code as a compliant method for the registration of financial instruments, France has opened the way for better projects that aim at creating better systems for the issuance and exchange of financial instruments for

1 Blockchain and Digital Identity, EU Blockchain Observatory and Forum, 2 May 2019.
2 Legally binding blockchain technology transactions, Deloitte
3 See Ordonnance n° 2016-520 du 28 avril 2016.
4 See Ordonnance n° 2017-1674 du 8 décembre 2017.

non-listed SMEs. It has also set the tone for a favourable, innovation-friendly ecosystem and led to experimentations on low-risk assets.[5]

TERRITORIALITY

As we have mentioned, blockchains, at least in most public, permissionless blockchain networks like Bitcoin, are not rooted in any specific location. Anyone with the necessary hardware and know-how, regardless of where they are, can operate a node. That can make it difficult to assign legal responsibility. Also, each network node may be subject to different legal requirements, and there is no "central administration" responsible for each distributed ledger, the nationality of which might act as an "anchor" in terms of regulation.

At the same time, permissionless blockchains are, by definition, open to anyone to participate in. This can be a problem in use cases, like financial services, where there are know-your-customer (KYC) or anti-money-laundering (AML) regulatory requirements.

To be clear, this is not the case for all blockchains. It is, at least in theory, possible to have public, permissionless blockchains where all nodes are located in one jurisdiction or even data centre, or that is managed by a legal entity established in one specific jurisdiction. Private, permissioned chains, for example those set up by a consortium, will also generally have a legal entity at their core and some way of vetting or identifying users.

That said, as a technology designed to enable collaboration among broad sets of stakeholders based on shared infrastructure, there is no doubt that blockchains will raise thorny issues of territoriality.

This makes cross-jurisdictional harmonisation important. That, in turn, requires regulators and lawmakers to collaborate across national borders to harmonise legal and regulatory regimes, while managing potential risks, including issues of monopolies and market manipulation. Addressing these would require significant legal and organisational changes and a mechanism for collaboration to ensure alignment.[6] [7]

On-chain conduct may, in certain circumstances, give rise to issues of tortious liability and non-contractual disputes. In a cross-border context, the issue of which is the applicable law to any such liability and non-contractual disputes can give rise to a number of challenges. This is because the law will often refer to the location where damage occurs. It may not be entirely clear in which country the damage occurs in relation to conduct on distributed ledgers.

From an EU perspective, the general rule under the Rome II Regulation, designed to help choose which laws apply to disputes within the EU, points to where the damage occurs or is likely to occur, to determine the applicable law in relation to non-contractual disputes.[8] In cyberspace, the determination of the place of damage may require a delict analysis approach, as evident from binding judicial

5 See also Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019, p. 282, Global Legal Group Ltd, 2018; and Regulation of cryptocurrency: France, Library of Congress.

6 M. Niforos, Blockchain: Opportunities for Private Enterprises in Emerging Markets, Chapter 7, IFC.

7 For a detailed analysis, see IBA Legal Policy & Research Unit Legal Paper Rule of Law Versus Rule of Code: A Blockchain-Driven Legal World.

8 Article 4.1, Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II).

precedent.[9]

Similar challenges emerge when considering territoriality aspects and court jurisdiction in relation to torts and non-contractual disputes. In determining the competent courts vis-à-vis tortious liability, the EU Brussels I regime generally points to the place where the harmful events occurred or may occur.[10] In applying the applicable legal rules to determine which courts have jurisdiction over a dispute, the Court of Justice of the EU has considered the place of the causal event to be identical to the place of domicile (or establishment) of the relevant information society service provider.[11]

The nature of blockchains may render it difficult to determine in what country a damage occurs as a result of conduct on blockchains. For this reason, we might need to revisit aspects of European private international law. With a view to achieve certainty as to the precise nature and scope of legal relationships on blockchains, a potential approach could be to develop existing legal tools further. This could mean revisiting the existing provisions of Rome II and Brussels I Recast, enabling parties to choose a governing law[12] and the courts having jurisdiction over any disputes,[13] respectively.

ENFORCEABILITY

1. Pseudonymity/Anonymity

Laws can only be effective if they can be enforced through penalties or sanctions against the lawbreakers. To do so, the law needs to be able to identify them. As we have seen, this is not always easy to do on a blockchain platform.

The potential for pseudonymity and, in some cases, full anonymity on blockchains has given rise in some circles to the impression that they can be used to create lawless zones for the benefit of criminals. While the potential is there, the truth so far has been different.

For one, the problem of using blockchain technology to evade legal responsibility is not an issue in private/corporate permissioned blockchain, where all actors are identifiable and accountability is easily determined.

Secondly, in the case of the majority of public permissionless blockchains, it is not true that users who violate the law on a blockchain are not identifiable or traceable. That's because the entries in the ledgers are immutable, providing an audit trail and evidence of wrongdoing. While not always identifiable at the moment of the transaction, given enough time and effort, many parties to a transaction can be unmasked. Therefore, at this point there is no question of total impunity for blockchain actors.

Thirdly, however, it can not be denied that some privacy-focused blockchains, for example Monero or ZCash, can provide bad actors with effective tools for true anonymity. It is important to note that in practice anonymous transactions are currently not widely used: Bitcoin and Ethereum, the most popular platforms, do not support anonymity.

9 See, for example, Case C-170/12, Peter Pinckney ECLI:EU:C:2013:635; Case C-523/10, Wintersteiger ECLI:EU:C:2012:220.
10 Article 7(3), Regulation (EU) 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast) (Brussels I Recast).
11 See, for example, Case C-441/13 Hejduk ECLI:EU:C:2015:28; C-360/12 Coty Germany ECLI:EU:C:2014:1318; C-523/10 Wintersteiger ECLI:EU:C:2012:220.
12 Article 14, REGULATION (EC) No 864/2007 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 July 2007 on the law applicable to non-contractual obligations (Rome II).
13 Article 25, Brussels I Recast, op. cit..

Governments also try to discourage the use of anonymization techniques in blockchain networks by, for example, imposing AML rules, thereby policing the gateway between the worlds of cryptocurrencies and fiat money (see also next section).

That said, while anonymisation does not pose a significant enforcement risk on public permissionless blockchains at the moment, should the use of anonymous blockchains spread significantly, it could become a problem.

It seems that providing states with identification tools (potentially under the control of courts or through the private sector on a payment basis) should be a minimum condition necessary for a state's ability to enforce the responsibility and thus to ensure the impact of the law on human behaviour in the blockchain space.

2. Enforcement access points

That said, if data and transactions on a blockchain are for some reasons not directly accessible to law enforcement or regulators, that does not make blockchains un-regulatable per se. Quite the contrary, as there are any number of "access points" that authorities could use to enforce rules. In her book Michele Finck (a member of the EU Observatory) discusses among other things the following options:[14]

ISPs: In the early days of the Internet, when it too was considered a lawless environment, regulators found that Internet Service Providers could serve as legal and regulatory access points. Since then they have among other things "forced" net neutrality laws on ISPs and have also been known to turn to ISPs to block illegal content. Something similar could in theory be done with blockchains. For example, authorities could require ISPs to block encrypted data or block specific transactions or traffic to/from specific apps or even nodes. As is the case with the Internet, these may not be perfect remedies: blocking is not always feasible, for example if users use services like Tor or VPNs, and users determined to make illegal transactions can easily switch locations to evade detection. Depending on the case, blocking data or transactions could also infringe on users' legitimate rights. Still, the option is there.

Miners: While in theory any participant can be a miner on a blockchain network, the computing resources necessary to make mining profitable, at least on energy-intensive proof-of-work blockchains, has to date favoured the rise of a small number of large mining pools, as we have seen with Bitcoin.[15] Such pools are generally identifiable, via direct or indirect means, and so can be addressed by the authorities. This is important because in blockchain networks, miners have a great deal of influence. Not only do they validate transactions, they can also influence the development of the protocol by accepting or refusing updates. This makes miners effective regulatory access points. Authorities could in theory force miners to make changes to the blockchain protocol or applications, they could use incentives to entice miners to only process "legal" transactions, or tax or otherwise penalise them if they do not. In the case of intransigent mining pools, at least on proof-of-work blockchains, governments could conceivably close down operations simply by shutting off

14 Michéle Finck, Blockchain Regulation and Governance in Europe, Cambridge, 2019.

15 See for instance: https://www.buybitcoinworldwide.com/mining/pools/.

BLOCKCHAIN TECHNOLOGY AND THE LAW

their power.

Core software developers: Most blockchain protocols rely on a set of core software developers who play a key role in designing, developing, maintaining and evolving the protocol. Today, these developers tend to be active publically and are therefore generally identifiable (the great exception being Bitcoin's Satoshi Nakamoto). Governments could therefore in theory address core developers as enforcement access points, potentially requiring them to make additions to the code, like backdoors, to help support legal and regulatory enforcement. Whether this is always practical or even advisable is a different question. Backdoors can weaken the security of an entire network, which is not necessarily in the interest of authorities. Developers tend to be located all over the world, making it difficult for authorities in a single jurisdiction to address them all. Core developers can also choose to move to friendlier jurisdictions or can be replaced by developers elsewhere. Similarly, addressing core developers may have the effect of forcing some of them underground. For governments interested in the healthy development of a blockchain industry, this is not necessarily desirable either.

End users: There is often a misconception that users of blockchain-based platforms are anonymous and therefore can act with impunity. Quite the contrary, platforms like Bitcoin offer pseudonymity at the most: while it can be difficult to identify users in real time, with enough effort it is becoming increasingly possible, by studying the ledger, to figure out who the parties to a transaction are. Unlike core developers, end users of blockchain platforms are not typically willing or able to change their location in favour of more lenient jurisdictions. This makes them attractive potential enforcement access points for the authorities. To an extent they already are: uploading illegal content to a blockchain is just as criminal an action as it is uploading it to any other type of online platform. If they wanted, authorities could extend this idea to ban the use of certain types of dApps or certain kinds of transactions. That said, users can be a difficult access point as well. First off, compared to miners or core developers, there are many, many more of them. Secondly, if certain types of decentralised transactions become highly desirable and take on the status of social norms, authorities may face a backlash if they try to ban them. Users also tend not to understand how the technology works. While it makes sense to hold individual users responsible for their own actions, it would not necessarily be feasible or practical to leverage them as access points for influencing protocol governance or any type of platform-wide decision.

Old and new intermediaries: Much more straightforward and logical would be to address intermediaries. For despite its claim as being a technology of disintermediation, most blockchain platforms still rely on a number of outside actors to function. These may be the traditional intermediaries, like banks, search engines or social media companies, which could for example be forced to block blockchain-related content,[16] or new intermediaries, like crypto exchanges, which can be forced to adhere to AML and similar regulations, or – as was the case with Coinbase[17] – to turn over customer data to tax authorities. While intermediaries can be very effective regulatory access points, as with any regulatory intervention, the authorities must balance

16 See for example: Twitter Will Ban ICO Ads Starting Tomorrow, CoinDesk, 26 March, 2018.
17 Coinbase tells 13,000 users their data will be sent to the IRS soon, The Verge, 26 February 2018.

the aims of the law against the potential for stifling innovation. An overly high regulatory burden on new types of intermediaries could make it difficult for them to compete with incumbents. If the authorities use incumbent intermediaries as the sole access points – for example, requiring that KYC/AML checks on a blockchain-based platform can only be performed by licensed banks – they could make it difficult for new entrants as well, and so perpetuate the status quo.

Governments as blockchain participants: Last but not least, governments can become access points themselves by participating in the blockchain ecosystem. They can run their own nodes and become miners. They can develop their own blockchains and cryptocurrencies. They can tax mining rigs or use market interventions, like subsidies or procurement policies, to support the blockchains they favour.

LIABILITY

The law consists of obligations and prohibitions of specific behaviour, and places a liability/responsibility on the person who fails to comply with it. The primary goal for which such a responsibility is imposed is to motivate/steer the behaviour of a person towards the direction desired by the legislators. Liability regulations also have a compensatory function: their purpose is to provide the injured person with the opportunity and source to obtain compensation for damages.

Today, the rules for attributing responsibility vary greatly depending on (i) who, (ii) to whom, (iii) what for and (iv) on what kind of consequences/pain a person is liable. The main kinds of liability in law systems usually include: criminal responsibility, administrative responsibility, contractual liability and tort liability. Partially separately regulated is the liability of board members towards the company. Also, many specific regulations and laws provide for special regulations on liability issues (e.g. the GDPR). At the EU level, the rules governing liability are only partially harmonised in some sectors.

In such a short report, it is not possible to even briefly present them all. Only some general comments concerning liability for breach of law or for causing damage, in connection with activities using blockchain technology, are provided below.

1. Liability of core software developers

As we have seen, core developers make attractive access points for the enforcement of laws and regulations. Considering their role in designing, developing and maintaining blockchain platforms, they are also accessible enforcement targets for questions of liability.

Indeed, we have been seeing more and more charges (or threats of charges) being brought against core blockchain developers on different legal bases. This has led to a sometimes heated debate around what are and what should be the responsibilities of core developers of open source code, especially dApps or public permissionless blockchain protocols. Should they be responsible, for example, for the fact that the code is used for illegal activities – say for creating and operating illegal exchanges? Should they be responsible for the fact that the code does not have features which could prevent illegal activities? Should they be responsible for creating open source code that supports anonymity?

These issues are not, however, new with

blockchain. As we have seen, problems with delineation and definition of obligations imposed on various digital space actors have arisen also in the Internet space (e.g. distinguishing what is the responsibility of internet service providers, search engines, application operators, website administrators and end users). Also, in the context of different roles of players in the blockchain space, a deeper discussion is needed on whether it is rational, feasible, enforceable and supportive of innovation to impose specific duties on specific actors. In general, it does not seem appropriate to charge core developers with responsibility for any unlawful use of an open source program merely because they are the creators of the tool. Blockchain open source software, similar to all other products, can be used to achieve good and evil goals.

However, it should also be remembered that in blockchain projects, core software developers are not necessarily just software developers working pro bono, but very often they are also (co-)founders of business projects. They themselves use the tool they have created, and under certain circumstances they can profit from the fact that the free tool they have created is used by an increasing number of people. Their profits often do not result from dividends or fees charged on transactions, but from an increase in the value of tokens financing the total or partial development of a business or from advisory services to a foundation which supports the development of the project. Core developers, as co-founders, often retain some tokens for themselves, so part of their profit depends on the success of the venture. Therefore, as entrepreneurs (and not only the creators of open source software) the scope of their responsibility is, and may be, much broader.

On the other hand, a core developer and (co) founder of a blockchain business project who has deployed software in the public space of permissionless blockchain(s), may partially or completely lose his or her influence over further functioning and development of the given project. Often, other actors in the blockchain network (e.g. other developers, miners, validators/nodes, users) become involved in the governance and management processes of such public permissionless blockchain-based projects too.

In practice, indicating the precise moment when the founder or co-founders of the projects, who in the initial phases were actively co-"managing" the project, are no longer responsible for its continuation (and for the related legal consequences) is very difficult. While it is easy to indicate the moment when a CEO leaves a company and the company delegates its responsibility to a successor, in the permissionless blockchain space there is no such clear moment. It should also be kept in mind that imposing extended responsibilities on core developers may drive some of them to escape into anonymity or discourage them from making an effort to innovate. One of the main reasons for the creation, by systems of law, of the legal construct of a "company" was the aim to create incentives for innovation by providing a tool to limit the liability of individuals related to risky innovative activity.

2. Tort liability (liability of network participants generally)

Tort law generally deals with issues of civil wrongs where one person can be held liable for damages caused to another.

As we have seen, while it is generally – but not always – possible to identify actors on a

blockchain network, this does require time and effort, and is therefore not always practical. This can in turn be an obstacle in enforcing liability (compensation) on actors in blockchain-based networks generally.

That said, it should be noted that the risk of failure to identify the person who caused the damage also exists in the real world. It is not related only to blockchains. Usually, the injured party does not have any influence on whether the damage is done by a person who is easily identifiable.

In some situations, governments have therefore decided to protect the injured/damaged party by other means, not only by relying on enforcing liability. For example, banks are obliged to create a pool of funds to cover damages to their clients caused by a bank insolvency. National health insurance systems cover the risk of personal injuries. Insurance companies are obliged to maintain an insurance fund which is liable to pay compensation to victims injured in road traffic accidents in cases when a driver has not been identified or has not been properly insured.

In the blockchain space we could envision similar solutions. The more serious risks related to damages caused by anonymous actors in the permissionless blockchain space, or risks borne by consumers, could be covered in a limited scope by creation of a common insurance system. Such measures would, however, make the whole system more expensive. Such means would not be necessary though if there were tools to identify all network actors. That would enable liability enforcement directly between the blockchain actors/users, without using an insurance institution as an intermediary.

DATA PROTECTION

The European Union has long looked to protect the personal data rights of its citizens. Its most recent and far-reaching effort in this regard has been the General Data Protection Regulation (GDPR), which became generally applicable in 2018.

While the GDPR is meant to take into account the significant developments in the online world over the past 25 years, it was written before the rise to prominence of blockchain and was therefore conceived with more traditional, centralised data-processing paradigms in mind. This has led to what many see as a number of tensions between blockchains and the GDPR. It is a very important issue for the blockchain industry, and one which we have already addressed in a previous paper.[18] We will therefore only summarise the main points here, and would point interested readers to that publication for a more in-depth discussion.

In summary, there are three main areas where there are tensions. In fully decentralised blockchains, it can be difficult to identify data controllers and processors as defined under GDPR, and hence enforce their obligations. This has to do with issues around jurisdiction and access points, among others, similar to those discussed above. Particularly in cases where it is difficult, or perhaps impossible, to identify a data controller, it can naturally be tricky to enforce the GDPR's requirements for the data controller.

There are also many questions and much debate around what it takes to anonymise personal data in such a way that it is

18 Op. Cit.

considered truly anonymous under the GDPR (where the bar for anonymisation is set very high). To take one example, the hashing of data cannot be considered to be an anonymisation technique in many circumstances.

Last but not least, blockchains can make it difficult to exercise some data subject rights as defined in the GDPR. This is most evident in the GDPR's well-known "right to be forgotten" provisions, as data that is recorded on a blockchain can generally not be altered or deleted. Other rights, however, can be problematic in a blockchain context too, including rights to the rectification of personal data, to know if one's data is being processed and – an issue with smart contracts – the right to be protected from decisions made only on the basis of automated data processing.

While these are all thorny issues, none of them seems insurmountable. Even today there are ways for blockchain projects to account for the GDPR, and we expect that over time policy makers, the courts and regulators will address the most outstanding issues and provide increasing clarity. Again, we refer the reader to our previous publication for more.

RISK TO FAIR COMPETITION

The realisation of blockchain's potential to generate novel ecosystems in trade, investment and commercial transactions could have a profound impact on markets and competition. The inherent characteristics of blockchain, particularly decentralisation and transparency, could lead to the enhancement of efficiencies and could lower boundaries for new competitors to enter old markets. At the same time, these attributes could also attract an increased risk of competition law infringements.

Some of the antitrust domains in which blockchain technology might have the most disruptive impact and give rise to the need for novel approaches to competition policy are the following:

Collusive conduct. Blockchain's full commercial potential will often be achieved through distributed ledgers to which actual or potential competitors participate. In that respect, blockchain could be deployed in a manner that facilitates, or even establishes, collusive conduct.

For example, competitors within a market may deploy one or more blockchains, whether as a new means of carrying out an existing economic activity or in creating a new market altogether. If the blockchain enables monitoring and penalising deviations of participants from agreements or concerted practices, it could be treated as a cartel.

Some competition enforcement agencies could suggest that tacit collusion might be facilitated through participation of competitors on a blockchain, without being in contact with each other or expressly agreeing to coordinate.

The exchange of information that reduces strategic uncertainty in the market can decrease incentives to compete and thus infringe competition law. Such information could relate to prices, customers, production, turnover, capacities, risks, investments and research.

The increased transparency advanced by blockchains could pose competition law infringement risks linked to information exchange. Seeing as information exchange

on a blockchain can generate efficiencies by improving contractibility, its incompatibility with Article 101 TFEU needs to be evaluated on a case-by-case basis.

Abuse of dominance. Abuse of a dominant position could also be a domain in which the inherent characteristics of blockchains could lead to competition concerns. Private blockchains, depending on their governance arrangements, could involve practices that result in the exclusion of market participants or create barriers to entry.

This would particularly be the case in relation to permissioned blockchains controlled jointly by existing members (gating), access to which is essential to compete. Refusals to give access could result in excluding new entrants in the relevant market and therefore attract competition enforcement scrutiny.

That said, regulatory intervention should certainly not hinder blockchain's ability to create efficiencies by creating regulatory barriers of entry into any market created on or driven by blockchains.

Whether competition policy would need to develop new norms or tools will depend on the nature and effects of the economic activity transacted on blockchains. No two cases are likely to be identical and a competition law assessment will depend entirely on the particular circumstances of a given blockchain and the relevant market.

Permissioned blockchains will likely have their consensus mechanism embedded in code. Seeing as the competition law framework implemented at an EU level and in the national legal orders is largely one of 'self-assessment' as to whether agreements and practices are compliant with competition law (as opposed to obtaining approval from competent authorities), undertakings may need to ensure that the code of their distributed ledgers, both in blockchain implementations they deploy and those they participate in, are compliant with applicable competition law.

Smart contracts and the law

WHAT IS A SMART CONTRACT?

The success of Bitcoin showed the world that it was possible to create digital cash by using a blockchain to enable strangers and adversaries to agree on and store trusted data.

It didn't take long for people to figure out that the same idea had much broader potential implications. Since computer programs are nothing but data (lists of instructions), people saw you could use a blockchain to allow strangers and even adversaries to share computer programs in such a way that they could be run decentrally and not under the control of (and hence subject to the manipulation of) any single party.

The race was then on to create blockchains that could handle general-purpose computing. The first major platform to introduce this capability was Ethereum, whose inventor, Vitalik Buterin, used the term "smart contract" to designate this capability. While he had good reason to use this term, this choice of wording has since been the cause of much confusion, as smart contracts are not necessarily contracts in the usual way we think of them (and Buterin has since publicly regretted his choice of terms).[1]

So what do we mean by the term smart contract? In the blockchain context, it generally means computer code that is stored on a blockchain and that can be accessed by one or more parties. These programs are often self-executing and make use of blockchain properties like tamper-resistance, decentralised processing, and the like.

Smart contracts can be used to do a lot of interesting things. They are used for tokenisation, and so are the engines behind cryptocurrencies and other digital assets. They can be used to code and automate business processes that can be shared and executed among multiple parties offering increased trust and reliability in the process, often with significant gains in efficiency and cost reduction. Similarly, you can use smart contracts to hard code agreements between parties involving value and other types of asset transfer, like escrow agreements or payment vs delivery or more complex agreements, and have them be very transparent and run automatically based on predetermined conditions, making it difficult or impossible for a party to back out.

If you add various kinds of "intelligence" to the smart contracts, whether simple if/then types of routines or complex, AI-driven decision making, you can make these programs highly autonomous: able to react to their environment and make decisions, including about buying and selling, on their own. In a similar way, you can "hard code" the rules for complex organisational structures into smart contracts, creating a trusted, immutable and tamper-resistant organisation where all members are held to the rules via the code. Such organisations can even be automated, creating decentralised autonomous organisations (DAOs) which, once set free in the wild, go about their business on their own with no human intervention.

Clearly if we are dealing with new kinds of

1 As posted on Twitter: https://twitter.com/vitalikbuterin/status/1051160932699770882?lang=en

currencies, new kinds of assets, and new kinds of organisation, we are dealing with new kinds of legal questions. Not all of these questions are explicit. For this reason, we think it makes sense to break up the discussion into two parts:

- **Smart legal contracts**, which are smart contracts on a blockchain that represent - or that would like to represent - a legal contract, along witht the issues that involves.
- **Smart contracts with legal implications**, which are artefacts/constructs based on smart technology that clearly have legal implications.

SMART LEGAL CONTRACTS

The idea of a smart legal contract is compelling. Since the invention of computers, people have wondered if you could you use the impartial logic of bits and bytes in the legal realm, to support and help improve the performance of fallible and corrupt humans in the pursuit of justice and the dream of fair, rules-based societies and economies. Or even completely replace them? Could code be law?

Yet, as we saw above when discussing the legal standing of blockchain registries, just because something works in code doesn't automatically give it legal standing. When it comes to the legality of smart contracts, here are some of the issues that arise.

1. Formal requirements

One rather simple issue that is, however, important and often overlooked involves whether or not smart legal contracts can meet the formal requirements laid out by the law for a legally binding agreement.

To take some simple examples: perhaps in a given jurisdiction a contract needs to be on paper or be notarised, or perhaps not. As an example, Swedish law normally accepts oral agreements as valid but only paper contracts when it comes to real estate. At the same time, unlike other countries, Swedish law does not require the use of notaries. Similarly, there may be requirements that a contract be in a language that both parties can understand. Can computer code be considered such a language? And if so, would we then have a need for "translations" of this language into others, like normal human language, and thereby also need rules for what constitutes a legally binding translation of a smart contract to say German, French or Italian?

2. Signing requirements

Another question affecting whether a smart contract is legally binding has to do with who "signed" it, and how this signature has been carried out.

As in the off-chain world, the signer needs to have the authority to sign. In the off-chain world organisations will often have designated people with signature authority. As digital documents, smart contracts need to be signed in some digital way. That brings up a number of problems.

As we saw above, to be legally valid in Europe under eIDAS, digital signatures on a blockchain must be verified by a TSP. An automated smart legal contract requiring such digital signatures will need to be able to ascertain if the signature is valid, if it refers to the correct person and, if so, if that person really has the authority to sign. In commercial settings, this could mean being

able to access company databases or some other reliable oracle. These, in turn, would need some sort of legal standing.

3. Immutability of smart contracts

The more "automated" a smart contract is, the trickier the legal issues can become.

To many, one of the great advantages of smart contracts is that they can be used to write "tamper-proof" agreements, meaning they cannot be changed after they are deployed. The advantage is that they will execute as written no matter what – holding, in theory, the parties to their commitments through the inexorable might of code.

Yet in such cases, what happens from a legal perspective if off-chain conditions change? There might be changes in the law, in applicable regulations, in the business environment, or other relevant spheres that would necessitate a change in the smart contract. What legal recourse would the parties have if the smart contract they have deployed cannot be accessed and modified?

Also, there are a lot of events that may occur in the off-chain world that affect, by law, the content of rights and obligations of the parties to the smart contract. If appropriate functionality is not included in the code to allow for the adoption of the changes in the legal contract, the smart contract could perform non-valid legal actions.

In a situation where, for any reason, the automatic execution of a legal contract by a smart contract breaches contractual obligations, the subsequent obligation will arise to make appropriate settlements between the parties (e.g. returning the transferred assets or paying their value). In B2B contractual relationships, the parties have broad competence to waive the obligations of such settlements. Professionals can therefore generally bear the risk of using smart contracts. However, limitations on obligations and liability are less effective in the case of B2C relationships.

Thus, despite the use of smart contracts, the obligation to make off-chain settlements may arise. The creditor (or potentially the consumer) would have to enforce such obligations in the real world. If no collateral for meeting obligations has been established, the primary and only tool for the enforcement of contractual liability is to use the judicial system. Creditors may sue the debtor before the court, but the decision of the court may be enforceable only if the debtor is an identifiable entity.

The conclusion is that the use of smart contracts does not resolve or eliminate the problem of breaches of contract, contractual liability and enforcement. The problem of the lack of available tools to easily identify actors on a blockchain-based network therefore arises again. It will require a solution, not only in relationships between blockchain players and state authorities, but also in vertical relations between the participants of the blockchain space. Otherwise, the current system of consumer (or any creditor) protection, currently based on judicial system and enforcement of liability, may no longer be effective.

4. Smart contract audits/quality assurance

There can also be serious issues if a smart contract has a flaw: a bug in an agreement that deals with asset transfers can be very

damaging indeed. Yet it need not necessarily be a bug. Depending on the complexity of the agreement, it can be extremely difficult to correctly or adequately encode contract terms. A smart contract might execute as written and yet still behave in ways not foreseen by its writers.

For this reason, smart contract "audits" – often complex, highly technical processes to check for the validity and viability of smart contract code – become important. That raises the question of whether such audits have to become requirements, or also need legal recognition of some kind to make a smart contract valid? This has yet to be decided.

5. Legal status, effect and enforceability of smart contracts generally

If the results of transacting on blockchains cannot come to manifest in the real world, and be capable of protection in the real world, their potential is significantly diminished. The act of transacting, even if devoid of requiring any element of trust, must result in an enforceable change over rights attaching to or deriving from the asset concerned, whether this is a token or is represented by a token. For the assets transacted on blockchains to exist in the real world, they should be vested with rights in rem.

It will likely prove desirable, if not imperative, that participants in blockchain networks can maintain confidence, legal certainty is at play vis-à-vis the binding nature of the contractual transactions on the blockchain. There is a plethora of possible choice of law approaches for the proprietary effects of transactions conducted on blockchains. Employing traditional rules, such as applying the law of the place in which the property or claim to property is situated on issues relating to rights or entitlement over crypto-assets would not be legally feasible. Neither would applying the law of the place where an "administrator" resides be workable, particularly in relation to public, permissionless blockchains. It is also clear that there is no panacea solution to this challenge, as different crypto-assets and varying levels of decentralisation would attract different types of solutions respectively. It could be that a solution whereby participants elect the governing law of the blockchain, as a fundamental aspect of the blockchain's creation and existence, will prove to be most effective.

SMART CONTRACTS WITH LEGAL IMPLICATIONS

Smart contracts in the larger sense of self-executing programs run on a blockchain can be used for more things than just agreements between parties. Many of these use cases result in blockchain artefacts that have legal implications. In this section we take a look at three of the most prevalent:

- Smart contracts representing assets in digital form.
- Smart contracts used to create decentralised autonomous organisations.
- Smart contracts that become autonomous agents.

1. Smart contracts representing assets in digital form

One of the most common uses of smart contracts is to represent assets of various kinds online. These might be financial assets or representations of physical assets, like real

SMART CONTRACTS AND THE LAW

estate or antique cars. They also might be natively digital assets, like crypto collectibles or cryptocurrencies (that is, assets that exist solely on-chain with no off-chain counterpart), or intangible assets like intellectual property or access rights.

While it is possible to represent assets digitally without smart contracts on a blockchain, through the process of tokenisation blockchains can be used to create digital assets with special characteristics: they can be made unique, unalterable, non-reproducible, non-counterfeitable and irrevocably transferable. In essence, these on-chain assets become "tangible". When you transfer ownership of them, it is akin to physically delivering the object, not just a promise to deliver the object. Through smart contract technology, such assets can also be programmable: for instance, bonds that automatically make dividend payments, and so on.

These properties combined with the general properties of blockchain-based platforms outlined above raise some interesting legal questions.

One issue when dealing with digital assets is to define what they are.[2]

This is not so much of a problem when dealing with digital assets that are representations of traditional assets. Here they simply take on the category of the underlying asset. Starting with Bitcoin, the advent of blockchain has, however, introduced new asset classes of native blockchain tokens of various kinds.

2 Please note: the discussion of digital financial assets and their relationship to financial regulation in particular, as well as the legal issues raised by blockchain-based financial markets, is vast. We are therefore planning to address this in a separate paper due out by the end of 2019. Here we provide an overview of some of the most important points.

The categorisation of these "crypto assets" has been a major concern in the blockchain and regulatory community for some time now. This is understandable: you can't police or regulate digital assets if you are unsure of their nature.

Presently there is no standard categorisation, with different jurisdictions proffering different opinions. There does seem to be a general consensus around the idea of three main general categories:

- **Payment/exchange/currency tokens** (virtual currencies or cryptocurrencies).
- **Investment tokens** (meant to raise capital and/or providing ownership and dividend rights of some kind).
- **Utility tokens** (enabling access to a specific product or service on the blockchain-based platform).

The situation, as said, is however far from settled. And it is made more difficult by the fact that certain tokens seem to have hybrid characteristics, and so do not easily fit in a single category.

We saw above that, because blockchains can be both decentralised and global, it can be difficult to ascertain which jurisdiction applies to a blockchain platform. This is of course also the case with digital assets issued on such platforms.

The pseudonymity and, in some cases, anonymity provided by blockchain platforms can also be a serious issue with digital assets, particularly digital financial assets. These properties can make it difficult to enforce Know Your Customer (KYC) and Anti Money Laundering (AML) laws, by making it hard to identify the asset owners. Nontransparency in terms of ownership can also make it difficult to properly assess and collect tax on digital assets.

SMART CONTRACTS AND THE LAW

On the other hand, honest digital asset owners can also have tax-related problems if they do not have clarity on what category their asset falls under.

Lack of transparency around the issuers of digital assets can also make it harder to protect investors from fraud. The ICO boom of 2017, for example, in which a large number of companies issued tokens without the typical communications and reporting requirements associated with regulated securities offerings, was a good example of how problematic this can be: a large number of such ICOs turned out to be scams. Pseudonymity and anonymity can also make it difficult for authorities to seize fraudulent assets.

The near-immediate transaction settlement and immutability properties of many blockchains, which is one of the main advantages of the technology, can also be problematic from a legal and regulatory perspective. For example, it can be difficult to enforce consumer protection regulations in a world where transactions are not reversible, which is a hindrance both when regulators are trying to protect consumers from fraudsters as well as when they are trying to protect them from themselves.

While much remains to be clarified, we believe that from today's perspective, smart contracts that represent digital assets can – and should – be written in such a way as to make them regulatory compliant.

This should certainly be the case with digital representations of traditional assets. For example, developers can and probably should code KYC and AML functionality if possible into smart contracts that allow for asset transfers (provided that would be applicable to the underlying asset). If you have a digital asset that represents intellectual property, for example a music copyright, then the smart contract can – and probably should – contain provisions for paying out royalties.

2. Smart contracts representing organisations (DAOs)

The disruptive potential of DLT is revealed when we look at the case of decentralised organisations (DO), and specifically at more or less autonomous, decentralised organisations (DAOs). DAO is a form of organization (entity) that "relies on blockchain technology and smart contracts as their primary source of governance".

We could observe that DAOs are not registered under any jurisdiction and do not rely on legally binding agreements and their enforcement. Instead they form "an interconnected system of technically enforced relationships" enabling even extremely large groups of people, as well as entities of any kind, from all over the world, to cooperate smoothly in the way determined in and executed by protocols of public permissionless blockchains or dApps.

A common goal of such cooperation is usually to deploy, keep operating and develop a distributed ledger of data (DLT) or a dApp. It enables anyone to use the blockchain or dApp. Operating distributed software enables each DAO community to potentially make a profit. Usually there are several groups inside each DAO community, with different functions (e.g. developers, miners, validators, nodes) and different kinds of profits (economic incentives). Economic incentives are employed in order to encourage the actions of the players within the system to maintain and develop the network or

SMART CONTRACTS AND THE LAW

dApp (or in other worlds: "to encourage desired properties to hold into the future").

Technological developments, business competition, changes to law systems or other events and processes happening in the off-chain world may create a strong desire inside a blockchain/dApp community (we can say: inside a DAO) to change the protocols or off-chain governance rules and habits. While the rules of governance included in the code are clear and very strict, the off-chain governance rules are usually unwritten, difficult to identify, and dependent on the actual strength of different groups inside the DAO.

No board or directors are appointed, though inside some communities informal leaders emerge. An important role is also played by the foundations (legal entities) focused on the blockchain's development. The changes to the protocol (often: forks) result from spontaneous decisions on the part of community members, or result from long off-chain debates, or even from off-chain agreements. Other, often unpredictable, factors could also have an influence on the development of off-chain governance rules and customs of a blockchain community. The personal scope of a DAO (for someone who is, at a certain point in time, a "member" of DAO and who is merely a user of an open source technical infrastructure) is unclear and could be highly disputable in many cases.

In the light of at least some legal systems, some DAOs can be qualified as an organisation based on a multilateral contract, depending on whether the minimum requirements needed for conclusion of a contract have been met, as indicated by applicable law(s). In some cases, such qualification may result from a partnership agreement (e.g. Cyprus law), civil law partnership agreement (German law, Polish law), unincorporated joint venture agreement or other type of agreement. An unambiguous legal qualification is not possible here due to the significant diversity in the governance rules and habits in scope of public permissionless blockchains and dApps. Each of these legal qualifications may result in acceptance of the broader or narrow scope of personal responsibility/liability of DAO members for the legal obligations attributed to the DAO.

Subject to the differences between legal systems, the qualification of a DAO as, for example, a civil law partnership may give rise to unlimited liability for all the DAO's obligations for all of the DAO "members" (partners), including all their assets, and including also a risk of imprisonment, if an applicable law system accepts such a type of civil law sanction. The possible corporate structure of a civil law partnership is very flexible and also covers such entities that have not fulfilled any registration requirements and have not established any central management body/board. At least in some jurisdictions, there is no need to formalise the structure of internal relations of partners. In the absence of a central management body/board, every partner (DAO "member") can play the role of a legal link ("legal interface") with the off-chain world. There are no high requirements for contributions, also since all partners are jointly and severally liable for all duties. These considerations show that a DAO does not necessarily present a completely new form of organisation of commercial activity.

However, up to now the legal institution of (civil law) partnership as a form of business organization was usually used for small-scale projects, with a small group of people involved

SMART CONTRACTS AND THE LAW

and a low risk level. DLT, however, has made it possible to smoothly operate global business projects with a huge number of participants.

Thus, despite the fact that some DAOs could be associated with existing types of contracts (especially partnerships or unincorporated joint ventures) or, at least, could be classified as a new type of multilateral agreement, there is a need to discuss a special regulation that should take into account the key role of technology in a DAO and the global nature of such an organisation as an intrinsic feature. It is worth discussing the regulation adopted by Maltese law, where the authorities require that verification and supervision is possible not only of the content of agreements concluded in a traditional form, but also the code/protocol itself, along with all of its changes.

Currently, a DAO's contractors/counterparties have to examine in each case the full, non-transparent, internal DAO governance structure, including the code content, in order to identify the legal nature of their counterparty. Even for state authorities this is a major challenge, not to mention the difficulties faced by the average entrepreneur or consumer. Clarification of the DAO's legal status is therefore desirable not only for the sake of the DAO members themselves, but primarily in the interest of DAO counterparties. They should be able to clearly identify who is the counterparty, instead of having to identify all its members (which can also be other DAOs) and to verify the DAO's governance of on-chain and off-chain rules and habits.

It is a matter for debate whether practical considerations require the acceptance of legal entity status to DAOs. It may be sufficient for a DAO to consider it to be an organisation, without legal personality, but with an ability to act as a party (counterparty) in legal relationships for/on behalf of all its members (as is the case in some companies without legal personality). However, for practical reasons the clear identification and indication of all a DAO's members by contractors/counterparties should not be required.

It is necessary to take into account the differences between DAOs (as an organisation of natural and legal persons which relies on DLT and smart contracts as their primary source of governance) and "pure" technological structures. Such an extreme autonomous solution is self-operated or operated by artificial intelligence, not controlled (both: DLT and artificial intelligence), directly or indirectly, by humans, and neither individuals nor legal entities take profits from it. Such an extreme autonomous solution, not being an organisation of people or legal entities, would not constitute a DAO. Attribution of legal personality to a DAO should not result in any case in accepting the legal personality of a "pure" technical infrastructure, however in practice it will become more and more difficult for authorities and all market players to identify, whether they are interacting with an infrastructure operated by a DAO (an organisation ultimately controlled, at least indirectly, by humans) or with a "purely" technical infrastructure, neither operated nor controlled by humans.

One of the key problems relating to DAOs is the fact that legal qualification of a DAO may differ significantly under different national regulations and there is no clear link to connect DAOs to one national law system. Usually, a DAO has no seat, no board, no central point of government and no place of operation relating to the territory of one state. Rather,

SMART CONTRACTS AND THE LAW

the DAO community is scattered around the world. In other words: a DAO can be nowhere and everywhere. The mere indication of the law applicable to assess the legal nature of a DAO, as well as the scope of liability of DAO members, faces huge legal uncertainty. It could be proposed that in this case the creditor (especially the injured party requesting compensation on the basis of tort law) should have the right to indicate the applicable law. However, the choice of law by the state authorities would not be a proper solution for applying public law or tax law requirements. Therefore, harmonisation of legal systems on a European and global level is highly and urgently desired.

The question is whether there is anything that could push decentralised communities of permissionless blockchains to register, in any state, as a business entity and to comply with the chosen legal system. Blockchain communities such as Bitcoin or Ethereum (which can be considered a DAO variant) have never registered themselves in any jurisdiction, not even in a "blockchain friendly" jurisdiction. It is thus highly probable that the DAOs not registered under any jurisdiction will continue to exist. This tendency may be reinforced when blockchains supporting anonymity become widespread. But this tendency could also be reduced by creating legal regulations for DAOs that are acceptable for some DAO communities.

If legal systems adapt their legal requirements in order to facilitate the "absorption" of global DAOs into the regulated area, then it can be expected that some members of blockchain communities would adapt at least some of the DAO (or their forks) to legal systems. This, in particular could happen for two reasons.

Firstly: incentives. Clarity of the legal status of a DAO and its members in the face of legal system(s) would significantly increase the attractiveness of a DAO to its users. It is always a great incentive for a public permissionless blockchain community to expand the number of its members and users. Currently, the dubious legal status of DAOs discourages many potential users from entering these communities.

Secondly: threats. Regardless of the frequent declarations of blockchain space participants on not being subjected to any law, almost every activity in blockchain space is subject to regulations of many law systems, albeit identifying which ones is highly disputable. The risk of joint and several liability of all DAO members for the whole project exists. This risk may motivate at least part of the DAO communities (in particular, on blockchains which do not support privacy) to use legal tools to limit their liability. This would require them to comply with the requirements of the legal systems.

Thus, the legal systems should be prepared for two equally likely scenarios. The first is the future of global DAOs registered in some jurisdiction and complying with the (adopted) legal rules; these DAOs will be an effective point of accountability and enforcement liability for other market actors and state authorities. To reinforce the chances for this scenario occuring it is necessary to create appropriate regulations, harmonised on a global level. The second scenario is the functioning of global DAOs not registered anywhere, not compliant with regulations, and providing different levels of privacy/anonymity (on a scale between easy identification and full anonymity).

The identifiability of actors in the blockchain space seems to be a condition of accountability for governance and enforcement of liability. It refers also to a DAO and to a DAO's "members". In case of a lack of a market player's ability to easily identify DAO members (which could be also other DAOs), alternative DAO liability systems could become accepted. For example, it would be possible to arrange insurance funds/pools (which could collect a small fee from each transaction made on a blockchain, gathered on a separate address from which payments could be triggered, e.g. by a court, up to a limited amount). Of course, such collective liability insurance schemes would increase the cost of blockchain transactions, but it could be a real solution to the challenges faced by market players (including consumers) with respect to the identification of DAO members and with respect to the enforcement of liability of a DAO and/or DAO members before the courts.

It should be emphasised that it is already practically possible (though still very difficult) to build global distributed and partially decentralised blockchain projects that are fully compliant and "reconciled" with legal systems, even on a global level. Such projects consist of private permissioned blockchains and centralised applications which are in operation on these blockchains. Their governance is based on multilateral, well-defined contractual agreements between all members of a consortia. Members of the consortia are fully identifiable to state authorities and other market players, and their legal relationships can easily be subjected to control by the supervisory authorities of different states.

However, they do not provide the kind of opportunities that are possible with public permissionless projects. Legal regulation of the DAOs should not be restrictive to the point of forcing DAOs on public permissionless blockchains to transform into corporate/private blockchains. First of all, society would lose, in that case, undeniable benefits and huge opportunities offered by the open formula of the permissionless network. Secondly, the DAOs would not cease to operate, but would transform into anonymous organisations or into pure technological infrastructures, not operated by humans and without a "kill switch".

3. Smart contracts acting as autonomous agents

We have seen that smart contracts can be designed to make decisions on their own and thus be partially or completely autonomous, while not necessarily being organisations. The behaviour of such autonomous agents raises interesting legal questions too.

One of the issues is whether there can be smart contracts that exist fully on-chain, or whether there must always, from a legal perspective, be some off-chain relationship between the parties to the contract. If the latter, then legal recourse would seem more possible. If not, it could get tricky. Similarly, if legal recourse is possible, that does not mean it is enforceable. Asset transfers, at least on most public, permissionless blockchains, are meant to be immediate and final. In such an environment it might be difficult to recover assets even with a legal judgement.

If a smart contract is taking decisions on its own then, depending on the circumstances, you might have to ask the question of whether or not such a contract has the legal capacity to do so. In other words, can software that

SMART CONTRACTS AND THE LAW

automatically executes an agreement be considered to be a contracting party or a representative of one, and if so, does it need to be its own legal person?

While there is already debate in the legal community around this question of the legal personhood of smart contracts, the issue is not necessarily acute now. As we start adding more real "brains" to smart contracts, for example through AI and machine learning, we may find ourselves using smart contracts to construct sophisticated autonomous agents that negotiate and enter into sophisticated agreements among themselves. This could make the question of legal personhood more pressing. If software can by itself be a party to a contract, how do you approach it for legal recourse? How should it handle liability if something goes wrong? As with DAOs, we could for instance envision a kind of insurance or minimum account that all such contracts hold to cover such cases, but that would likely mean making such requirements legally binding and ensuring they are coded in. And would we need a new legal construct, perhaps the idea of an "electronic person", to get this done?

The answers to such questions are important. There is always a possibility that a smart contract has a flaw, that the integrity of the blockchain is corrupted. In these situations questions of liability immediately arise, as has been set out above, putting coders, miners and other stakeholders at risk. To promote decentralised forms of cooperation on a DLT as means to develop commercial ventures, the cooperating entities - be they private or public - may wish to run the blockchain/DLT and use applications on top through a legal vehicle. This can be a for-profit company (e.g.: LLP, GmBH, Société Anonyme) or a not-for-profit legal vehicle (e.g. foundation). Whatever the choice, implications for liability emerge. The choice of the legal vehicle and its registration also have immediate fiscal repercussions. It has so far not been explored whether legal vehicles available under national regimes suffice to serve as underpinning autonomous smart contracts and other forms of decentralised DLT co-operation that operate cross-border across regions and continents, or whether a specific new legal vehicle of a transnational nature would be required.

Conclusion and recommendations

As blockchain technology becomes more widely used in support of new types of decentralised applications and platforms, lawmakers and regulators will increasingly find themselves faced with challenging questions. These challenges are healthy and to be welcomed as part of the natural processes of change in society. The law has great experience in successfully adapting to this kind of change, if often at its own pace. We do not think things should or will be any different for blockchain.

With this in mind, we would like to end with a few general thoughts and recommendations for how policy makers might go about this adaptation over the short to mid term.

1. Craft simple yet usable definitions of the technology

A simple but potentially quite useful first step would be for policy makers to clearly define what blockchains and smart contracts are under the law at the European level in order to have a shared definition for EU and Member State regulators. Considering how young the technology is, this definition does not need to be overly precise. It only needs to be workable, making it easier to add blockchain to existing laws by being able to reference this common definition. France can provide a good example here. In 2016 and 2017 (see above), when the country first adapted its laws to allow the registration of certain securities on distributed ledgers, it also provided a legal definition.[1] This has made it easier subsequently to add blockchain-based registries to other legislation. Similarly, other concepts could be defined including digital assets, DAOs, token issuances, smart contracts.

2. Communicate legal interpretations as broadly as possible

When blockchain is added into a law, or when a binding or highly certain interpretation of the law with regards to blockchain is reached, we think it is worthwhile for authorities to make an extra effort to communicate this to the wider community. For certain regulations such as eIDAS or the GDPR, a shared understanding can easily be reached and widely communicated, as we at the EU Observatory and Forum have tried to do in the past. Continuing such efforts in future, through various channels, could be of immense use to the community.

3. Choose the right regulatory approaches for the question at hand

When it comes to regulating new technologies like blockchain, regulators can choose from three basic approaches, each of which has its own advantages and disadvantages. They can for instance apply existing laws and regulations as they stand now to the new case. This has the advantage of simplicity, but in squeezing a new phenomenon into old requirements, regulators could run the risk of negating or watering down those aspects of blockchain that are truly innovative. A second approach is to amend existing laws to take into account what makes the new case special. This can be a pragmatic way forward, though it runs the risk of creating new loopholes, perhaps with unintended consequences. Finally, regulators can craft completely new, ad-hoc rules and

1 Dispositif d'Enregistrement Electronique Partagé (DEEP) in French. See: Gide.

CONCLUSION AND RECOMMENDATIONS

regulations for specific use cases. While flexible and innovation friendly, considering the speed of innovation and the rapid appearance of new use cases, regulators may find it difficult to keep up, or may find they are creating a confusing jungle of bespoke, even potentially conflicting, new rules. Our point is that there is no right answer, but rather that clarity on the different ways to approach blockchain regulation can be a good tool in helping policy makers strike the necessary balance between protection and innovation that they strive for.

4. Harmonise the law and interpretations of it

Whatever approach individual regulators take, we think it crucial that blockchain and smart contract regulation be as harmonised as possible throughout the EU. That means sharing definitions – and where possible sharing regulations themselves – as well as to the extent possible sharing common interpretations. Blockchain technology and its attendant use cases are international by nature. To be effective across borders, blockchain law and regulation in Europe needs to be aligned across the bloc's borders as well.

5. Help policy makers develop an understanding of the technology

Getting it right will require the respective authorities and the full ecosystem to understand this new technology and what can (and cannot) be achieved with it. We think education of policy makers is particularly important, and worth the extra effort. Education, training, hands-on experience and exposure to the technology and the ecosystem are the best way to provide regulators the tools they need to make the best decisions. We encourage the EU to continue with education efforts in the spirit of the EU Blockchain Observatory & Forum, as well as efforts to bring the policy and blockchain communities together, as it is doing with public-private partnerships like INATBA. In this way they can foster a pan-European understanding of the issues, and so foster more unified and effective decision-making.[2]

6. Work on high-impact use cases first

With so much to do, setting priorities will be key. While it can be tempting to attack all problems simultaneously, we recommend beginning with those use cases where there is already a great deal of activity and hence the largest potential short- to mid-term impact. In our opinion that would encompass the regulatory questions around digital assets as well as bringing clarity to blockchain and the GDPR. For other areas, we think authorities can take their time (see next bullet). This both on resource grounds and because those use cases are still very new. In our opinion, it would be wiser to keep an eye on developments but not necessarily intervene until these use cases mature. That said, we believe that the EU could and should support efforts by the industry to self-regulate – often an effective approach in the early stages of a new technology.

7. Closely monitor developments in less mature use cases and encourage self-regulation

As regulators know all too well, intervening too early in novel use cases can be counterproductive. In less mature blockchain use cases, for example questions around DAOs, we believe that the EU would profit from a wait-and-see approach, keeping a close eye on developments while the use cases mature. That said, when it comes to new use cases regulators can always support efforts by the industry to

2 This is particularly important in relation to eIDAS where national authorities will have an increasing number of trust service providers willing to use blockchain. Authorities need to develop the skills and frameworks required to certify those solutions.

CONCLUSION AND RECOMMENDATIONS

self-regulate. This is often an effective and prudent approach in the early stages of a new technology, considering the relatively small size of these areas.

8. Make use of blockchain as a regulatory tool

Last but not least, we think an excellent way for regulators to help monitor and regulate the industry is to get involved themselves. This not only has benefits in terms of education and, as we wrote above, as an indirect method of regulation through helping to shape the new ecosystem. Blockchain also offers potentially powerful new regulatory tools. For example, regulators could plug themselves into new blockchain-based platforms as they come online, unleashing new opportunities to improve the efficacy but also efficiency of their operations - including potentially with real-time regulatory monitoring and intervention capabilities. By "getting their hands dirty" now with the technology, regulators will be well placed to take advantage of the opportunities it offers them as these opportunities arise.

Appendix – Blockchain Terminology

What is a blockchain?
Blockchain is one of the major technological breakthroughs of the past decade. A technology that allows large groups of people and organisations to reach agreement on and permanently record information without a central authority, it has been recognised as an important tool for building a fair, inclusive, secure and democratic digital economy. This has significant implications for how we think about many of our economic, social and political institutions.

How does it work?
At its core, blockchain is a shared, peer-to-peer database. While there are currently several different kinds of blockchains in existence, they share certain functional characteristics. They generally include a means for nodes on the network to communicate directly with each other. They have a mechanism for nodes on the network to propose the addition of information to the database, usually in the form of some transaction, and a consensus mechanism by which the network can validate what is the agreed-upon version of the database.

Blockchain gets its name from the fact that data is stored in groups known as blocks, and that each validated block is cryptographically sealed to the previous block, forming an ever-growing chain of data. Instead of being stored in a central location, all the nodes in the network share an identical copy of the blockchain, continuously updating it as new valid blocks are added.

What is it used for?
Blockchain is a technology that can be used to decentralise and automate processes in a large number of contexts. The attributes of blockchain allow for large numbers of individuals or entities, whether collaborators or competitors, to come to a consensus on information and immutably store it. For this reason, blockchain has been described as a "trust machine".

APPENDIX – BLOCKCHAIN TERMINOLOGY

The potential use cases for blockchain are vast. People are looking at blockchain technology to disrupt most industries, including from automotive, banking, education, energy and e-government to healthcare, insurance, law, music, art, real estate and travel. While blockchain is definitely not the solution for every problem, smart contract automation and disintermediation enable reduced costs, lower risks of errors and fraud and drastically improved speed and experience in many processes.

Glossary

The vocabulary used in the context of blockchains is quite specific and can be hard to understand. Here are the essential concepts you should know in order to navigate this breakthrough technology:

- **Node:** A node is a computer running specific software which allows that computer to process and communicate pieces of information to other nodes. In blockchains, each node stores a copy of the ledger and information is relayed from peer node to peer node until transmitted to all nodes in the network.
- **Signature:** Signing a message or a transaction consists in encrypting data using a pair of asymmetric keys. Asymmetric cryptography allows someone to interchangeably use one key for encrypting and the other key for decrypting. Data is encrypted using the private key and can be decrypted by third-party actors using the public key to verify the message was sent by the holder of the private key.
- **Transaction:** Transactions are the most granular piece of information that can be shared among a blockchain network. They are generated by users and include information such as the value of the transfer, address of the receiver and data payload. Before sending a transaction to the network, a user signs its contents by using a cryptographic private key. By controlling the validity of signatures, nodes can figure out who is the sender of a transaction and ensure that the transaction content has not been manipulated while being transmitted over the network.
- **Hash:** A hash is the result of a function that transforms data into a unique, fixed-length digest that cannot be reversed to produce the input. It can be viewed as the digital version of a fingerprint, for any type of data.
- **Block:** A block is the data structure used in blockchains to group transactions. In addition to transactions, blocks include other elements such as the hash of the previous block and a timestamp.
- **Smart contract:** Smart contracts are pieces of code stored on the blockchain that will self-execute once deployed, thus leveraging the trust and security of the blockchain network. They allow users

APPENDIX – BLOCKCHAIN TERMINOLOGY

to automate business logic and therefore enhance or completely redesign business processes and services.

- **Token:** Tokens are a type of digital asset that can be tracked or transferred on a blockchain. Tokens are often used as a digital representation of assets like commodities, stocks and even physical products. Tokens are also used to incentivise actors in maintaining and securing blockchain networks.
- **Consensus algorithm:** Consensus algorithms ensure convergence towards a single, immutable version of the ledger. They allow actors on the network to agree on the content recorded on the blockchain, taking into consideration the fact that some actors can be faulty or malicious. This can be achieved by various means depending on the specific needs. The most famous consensus algorithms include proof-of-work, proof-of-stake and proof-of-authority.
- **Validator nodes:** Validator nodes are specific nodes in a network that are responsible for constituting blocks and broadcasting these blocks with the network. To create a valid new block they have to follow the exact rules specified by the consensus algorithm.

Learn more about blockchain by watching a recording of our Ask me Anything session.