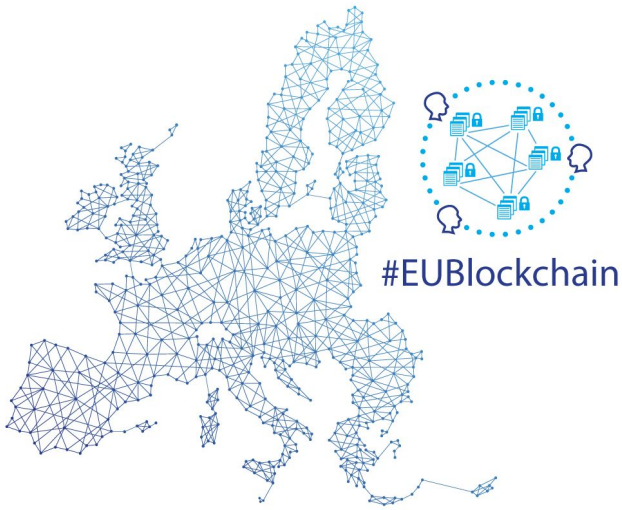
EU Blockchain Observatory and Forum

An initiative of the European Commission

EU BLOCKCHAIN OBSERVATORY & FORUM

Workshop Report - Legal Recognition of Blockchains & Smart Contracts Paris, 12 December, 2018



By the European Commission, Directorate-General of Communications Networks, Content & Technology.

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

Reproduction is authorised provided the source is acknowledged.

Author: Tom Lyons

Published on 20 December, 2018

Comments and inquiries may be addressed to the following email: info@eublockchainforum.eu

Table of Contents

Context

No digital technology is an island unto itself, existing only in the realm of bits and bytes. Quite the contrary, as with any tool our digital technologies are meant to serve human ends. That means they cannot help but intersect with the analog – and very human – world of the law and regulation.

This is certainly the case with blockchain. By enabling new, often decentralised, means for human transactions and agreements, blockchain has the potential to transform or disrupt important social and economic institutions. Not surprisingly, this raises a number of interesting and thorny legal and regulatory issues.

Shedding light on some of these problems was the object of the sixth European Union Blockchain Observatory & Forum workshop, held in Paris on 12 December, 2018. Below we present some highlights of the discussion. Links to further resources, including the slides and videos from the day, are included at the end of the document.

Introduction to the day

- Nadia Filali welcomed guests on behalf of Caisse de Dépots
- Peteris Zilgalvis from DG CONNECT then did a short introduction, underscoring the European Commission's appreciation of the work of the EU Observatory & Forum as an input for policy makers, and outlining the other significant EU blockchain-related initiatives, including giving an update on the European Blockchain Partnership.
- He also underscored that, while there wouldn't be any blockchain-specific regulations, as EU law is technology neutral, the Commission was interested in seeing if there potentially needed to be adjustments to remove barriers to blockchain, including for instance to support cross-border recognition of smart contracts across or bring clarity to issues around tokenisation.
- Ken Timsit from ConsenSys then gave a short overview of the work of the Observatory to date, and introduced the agenda for the day.

Panel discussion: Legal and regulatory framework: actions and harmonization for legal certainty at the EU level

Peteris Zilgalvis (DG CNECT)
Nadia Filali (LaBChain Consortium, Caisse des dépôts)
Anne Choné (ESMA)

Stephen McCarthy (Malta Digital Innovation Authority)
Domitille Dessertine (Autorité des Marchés Financiers)
Claire Pion (ConsenSys)
Moderator: Susan Poole

- What is the role of legal and regulatory framework and why is legal certainty so important?
- The law for decentralised technologies, blockchain but also things like 3D printing, robotics, is different as no single entity is in control. There can be two approaches: use principle-based regulation based on existing legislation or move to something more like a US-style Millenium Act for blockchain, enabling smart contracts or tokenisation.
- Legal certainty is important for application developers, who want to know that their investment today in the technology won't be illegal tomorrow, as well as for consumers and end users, who want to understand their rights and obligations with this new technology and its attendant platforms.
- It is important for regulators and innovators to work together, as was done for example with LiquidShare in France. There is much precedent for this though there are extra difficulties with decentralised technologies that catalyse new business models.
- There is a great amount of interest and discussion in regulatory circles about crypto assets in general, and specifically ICOs, at the moment, but few concrete results. These can be expected to come over the course of the year.
- This is however a very new ecosystem with a wide variety of new business models, so the challenge is to find out how and to what extent these models match with existing rules and then where the gaps are. Issues in Europe for ICOs include to what extent do issuances fall for example under MiFID, what are the proper disclosure procedures, what are issuers around custody services, settlement finality, liability.
- There are many issues outside the financial sector that are also important, for example tax, identity, legal status of e-signatures, e-voting, liability.
- It is important to have common terminology at an EU level to ensure we have a common understanding about what we are talking about.
- For crypto assets regulatory priorities include frameworks for primary and secondary markets, and fighting fraud.

Panel discussion: Legal recognition of smart contracts and use cases

Primavera de Filippi (CNRS)
Michèle Finck (Max Planck I.)
Benedikt Schuppli (Lexon Foundation)
Robert Herian (Open University)
Nina Siedler (DWF)

Moderator: Susan Poole

- There is a question of what regulations apply now to the transfer of digital assets on blockchain. It is broader than smart contracts, there are also huge regulatory vacuums in terms of secondary markets. Many crypto asset exchanges are black boxes and market abuse seems to be quite common.
- There are also private/civil law implications of crypto asset transfers that are often overlooked in the discussion at the moment.
- One issue with crypto assets is that their usage can change as they are transferred, meaning that their regulatory treatment would need to change based on context.
- The question of asset transfer is also generally one that falls under national, not EU, law. This also raises complications for crypto assets, which generally know no national boundaries.
- There are also conflicts between what happens on the technical side in crypto asset transfers and how this is seen legally. For example, there are some smart contract situations in which a crypto asset is held in the contract itself for a time, and not by any of the counterparties to that contract. There are those who say in such a case the crypto asset legally belongs to the contract, which however is not a legal entity. But the law sees rather that such assets must belong to some legal entity. Some in the community want the smart contract to be its own legal entity.
- When looking at smart contracts, there is often a discrepancy between what is happening on the technical level and what is happening on the legal level. When you interact on the Internet the Internet is just the medium for counterparties to interact. The problem comes when you have smart contracts that are autonomous and so only controlled by the code, especially if the counterparties are anonymous or pseudonymous.
- There is a counterargument that smart contracts do not need a special legal framework as underneath such contracts is a “meeting of the minds” that can be discerned behind and outside of the code. The constraints on legally binding smart contracts do not necessarily come from the law but from the technical side.
- There are lots of questions around GDPR Article 22, which sets out qualified prohibitions on people being exposed to decisions made solely as a result of automated data processing. This definitely applies to smart contracts, although Art 22 is not a blanket prohibition, but rather has conditions.
- There are also frictions with consumer protection laws, for example revocation rights or in some cases requirements to provide an offer in writing, and others that do not necessarily fit in with blockchain-based processes.
- The question of liability is also complex: what happens if there is a bug in the smart contract? Is the developer liable? And if a smart contract is audited and certified, then is the auditor liable? Are the auditors providing insurance? The question is how we deal with risk in this arena.
- The legal system wants accountability. The legal system is conceptualised to not allow a vacuum, so it will try to pierce the technological veil to find those who are accountable.

Yet there are practical problems to allocating liability, as there are so many actors involved: miners, validators, pseudonymous actors, etc. So it is often difficult to allocate liability. This is a tension.

- There are many interesting questions around decentralised autonomous organisations (DAOs), for example if they need a specific, new type of legal personality, what jurisdictions apply especially if you don't know the location of all the participants, what kind of legal constructions do you need if the DAO is going to receive and manage assets, etc.

Working sessions

The second half of the day was devoted to a working session with general discussion among the group of invited participants. This in turn was broken down in to two parts:

Legal recognition of smart contracts and use cases: potential interpretations

- First question was about how to attribute liability in different scenarios, for example if a user is directly interacting with one or more smart contracts, what happens if something goes wrong, or what happens if you interact with a smart contract through a platform or some intermediary?
- One opinion was that there was not much difference with how it is handled today. You can have contracts today that for example rely on some outside data source, and if something goes wrong with the data source, there are resolution mechanisms, usually agreed to beforehand by the parties.
- But it is not always an oracle issue. If there is an error in the contract code that someone can exploit for their own gain or to break the law, how is that to be handled? Would the developer be considered liable?
- If there is a centralised entity providing the service, even if there is a smart contract involved, then question of liability should be pretty straightforward. The problem arises when you have some kind of decentralised application that is let loose in the wild, operated by peers, and that people make use of: is that for example a partnership?
- You need to know who is doing what: what is the company doing, what are the developers doing, who is the user, etc. That will help settle liability issues. If it is a cybersecurity issue, that could be the developers. If it is a service issue, that could be the service providers, etc.
- One opinion is that there isn't much difference between a smart contract and other software tools, which are generally provided "as is". The same questions of liability should apply.
- One way to deal with this, and one thing that is missing for the time being in the blockchain community, is the use of comprehensive terms and conditions to which users

agree and which would then apply and presumably handle liability questions. Then this becomes an issue of ensuring users have the necessary information about risks.

- Another opinion is that, while there seem to be members of the blockchain community who believe that they can get away with anything using anonymous smart contracts, the truth is that if something goes wrong, the law will always find someone to whom to assign liability.
- Another opinion was that, unless we are dealing with completely autonomous contracts developed by AI, it is hard to see how liability can be assigned to the contract developer. There are always contracting parties who have initiated the process, and liability can be traced back to them. Otherwise developers will need to start taking out liability insurance.
- There was a question if there was a better way to build trust in this technology besides terms and conditions, which people generally don't read or understand anyway.
- One promise of blockchain is to empower the individual, for example by giving individuals full control over their assets through private keys. But with this empowerment comes responsibility, for example for security.
- In general, it seems we are not operating in a world of a complete regulatory vacuum, but we may need clarifications of specifics.
- When dealing with data oracles, you generally have recourse to existing law. The oracle has the accountability, which may be mitigated through service level agreements.
- There may also be issues with the availability of remedial measures in a blockchain environment, for example restitution of assets or unjust enrichment.
- There was one opinion that smart contracts are not contracts at all: they are simply code that provides some transactional capabilities based on intrinsic or extrinsic conditions. Behind the code there are always people whose intention it is to agree on something.
- A useful distinction is between weak and strong smart contracts. Weak smart contracts are those that can be modified by the parties. Strong ones cannot. But if you have weak smart contracts then there is no advantage to it being a smart contract. There is no innovation there.
- Indeed, terminology is important. For example the term smart contract itself. It can be questioned whether as they exist today they are either contracts or smart at all. But with improvements in AI we can expect them to get smarter, and start transacting directly with each other. That clouds the picture.
- While for many clearly code cannot be law, things can get complicated when it is the intention of the parties to a smart contract to automatically execute an agreement, but then the intention of the counterparties is somehow misunderstood and incorrectly reflected in the code.
- Another important and thorny issue is the question of liability in DAOs, particularly public ones not related to any registered legal entity. Another issue with DAOs currently is that they purport to substitute for current corporate governance structures, but it isn't always clear what they are actually substituting. Legal jurisdiction can also be difficult to determine.
- For DAOs it is important to clarify where existing laws may apply, and to identify where there are gaps, if any. It was also pointed out that many people may turn to DAOs

precisely because they do not seek the cover of any legal entity. On the other hand, this is not always easy to get away from: in Germany, for instance, there is a default legal entity if parties do not choose one themselves. This puts unlimited liability on the parties, so there is a benefit to seeking the cover of a legal entity in many cases. Indeed, this question of settling and limiting liability lies at the heart of much contract law.

- When discussing the legal value of a blockchain-based proof, we need to take into acount eIDAS. The question is whether eIDAS's there levels of signatures are sufficient to make transactions legally binding in a blockchain context. Generally the feeling was that this was to be considered on a case-by-case basis.
- When discussing blockchain and the transfer of digital assets, a major question is how do we classify digital assets. The general consensus in the community (though by no means universal) is that there are three basic types of tokens: a) payment, security and utility. While this is generally accepted, many tokens have a hybrid nature, like a utility token that is traded on exchanges before the platform is live. So here too you need to look at things on a case-by-case basis.

Recommendations for an attractive legal and regulatory framework in the EU

The second part of the working session entailed a discussion of recommendations for the EU. Based on this and the discussions of the whole day, the following conclusions could be drawn:

- Where existing frameworks should - generally - suffice
    - Legal recognition of smart contracts
        - The term "smart contract", while it has become established, has lead to a certain amount of confusion. In most cases smart contracts are not contracts in the legal sense but rather the expression in code of a business process or agreement between counterparties, generally with the intention of facilitating automated execution of the agreement.
        - As such, we do not anticipate the need for specific smart contract law or regulation. Rather, the legal and regulatory treatment of smart contracts must be handled on a case-by-case basis taking into consideration the "off-chain" relationships and situation among the counterparties.
    - Qualification and categorisation of digital assets
        - Blockchain-based cryptographic tokens are used in a variety of ways. There is a need for a clear framework to categorise such tokens. We believe there are three main categories:
            - Payment tokens
            - Security tokens
            - Utility tokens

        - Once tokens are properly categorised, it should be possible to map them to existing frameworks, for example current financial, currency, consumer or investor protection regulations.
        - There will be cases in which certain tokens have a hybrid function; in such cases we will need clarification as to their legal and regulatory treatment
    - Tax and accounting treatment of digital assets
        - There currently is uncertainty about the tax and accounting treatment of blockchain-based digital assets.
        - Once tokens are clearly categorised, it should be possible to apply the appropriate existing tax and accounting frameworks to them.
- Where new frameworks will likely be necessary
    - Decentralised autonomous organisations (DAOs)
        - Blockchain technology allows for new types of governing structures for organisations, often by allowing for automation of much if not all of the governance activities in the form of decentralised autonomous organisations (DAOs).
        - We believe that certain kinds of DAOs could represent a new organisational form that might require the creation of a new type of legal personality and with it new legal and regulatory frameworks. This is still under debate.

Appendix

Workshop slides

- Full day presentation

Workshop videos

- Videos from this and all other workshops can be found on the EU Observatory website under reports
- Videos specific to this workshop:
  - Part 1 Introductions
  - Part 2 First Panel
  - Part 3 Second Panel
  - Part 4 Working sessions

Official agenda

9:00	*Welcome coffee*
9:30	Introduction of the day - Agenda & Objectives of the day
9:40	Panel discussion Legal and regulatory framework: actions and harmonization for legal certainty at the EU level
11:20	Presentations
12:00-13:15	*Lunch Break*
13:15	Working session - Legal recognition of smart contracts and use cases: potential interpretations (invitation only)
14:30	Working Session - Recommendations for an attractive legal and regulatory framework in the EU (invitation only)
15:45	Conclusion