

Contracts and smart contracts

Giovanni Sartor

European University Institute, Cirsfid-University of Bologna

The concept of a contract

Draft Common Frame of Reference for European Private law (II.I)

1. A contract is an agreement which is intended to give rise to a binding legal relationship or to have some other legal effect. It is a bilateral or multilateral juridical act.
2. A juridical act is any statement or agreement, whether express or implied

Principles, Definitions and Model Rules of European Private Law

Draft Common Frame of Reference (DCFR)

Outline Edition

Prepared by the
Study Group on a European Civil Code
and the
Research Group on EC Private Law (Acquis Group)
Based in part on a revised version of the Principles of European Contract Law

Edited by
Christian von Bar, Eric Clive and Hans Schulte-Nölke
and
Hugh Beale, Johnny Herre, Jérôme Huet, Matthias Störme,
Stephen Swann, Paul Varul, Anna Veneziano and Fryderyk Zoll


sellier.
european law
publishers

The effects of a contract

II . – 1:102: Party autonomy

(1) Parties are free to make a contract or other juridical act and to determine its contents, subject to any applicable mandatory rules.

II . – 1:103: Binding effect

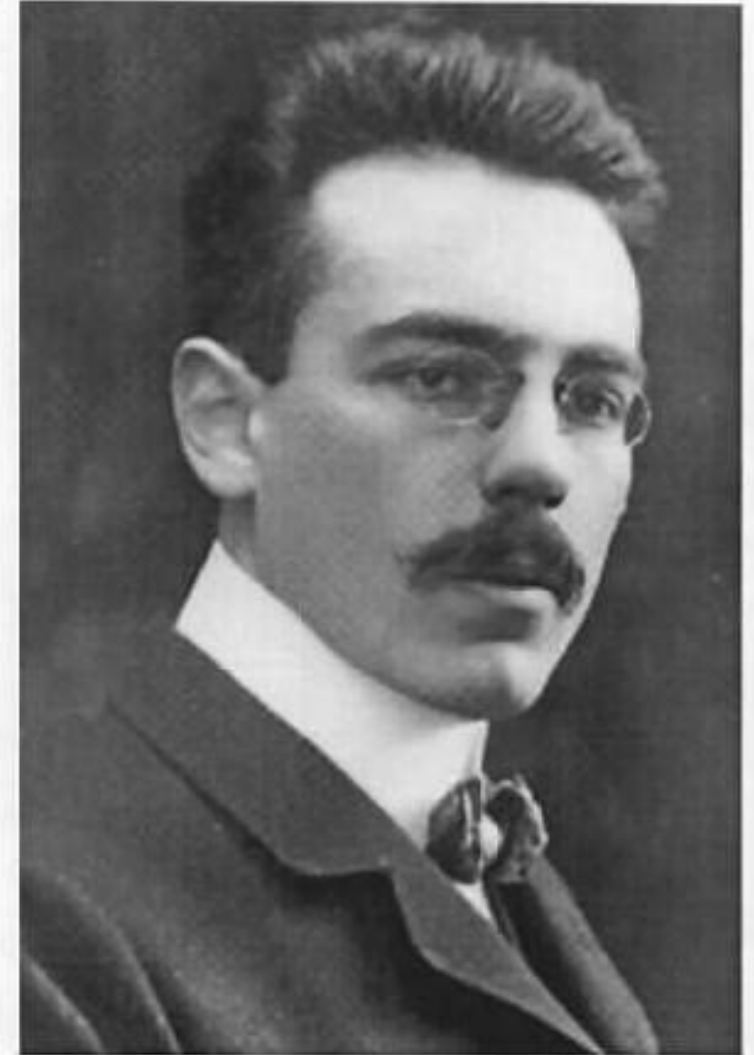
(1) A valid contract is binding on the parties

(3) This Article does not prevent modification or termination of any resulting right or obligation ... as provided by law.



What is a contract

- An institutional act
 - The parties declare their intention to achieve a certain legal results (through their declaration)
 - The law recognizes this intention, i.e., it makes it so that the declaration (the promise) realizes its content.



Adolf Reinach (1883 -1917)

Examples

- A sale
 - Titius and Gaia declare that Titius sells to Gaia his car, for 2000 Euros (i.e., that the ownership Titius's car is transferred to Gaia, and that Gaia acquires the obligation to pay 2000 Euros to Titius)
 - As a consequence of the declaration (plus delivery, if needed) the car no longer belongs to Titius but to Gaia, and Gaia has the obligation to pay 2000 to Titius
- A future contract
 - Titius buys from Gaia a foreign exchange future, for Euro 100,000, at \$1.250/€. In one month time,
 - if the value of the dollar in euro has increased by x , Gaia will be obliged to pay Titius the difference in the value of the dollars ($x*125.000$);
 - if the value has decreased, Titius will be obliged to pay Gaia the difference

The law and the contract

- The contract produces the declared changes only if legally valid
- The law
 - may deny validity to certain clauses
 - may establish effects of the contract that were not agreed by the parties (e.g., consumer's power to withdraw from an online sale, warranties, etc.)
 - May establishes good faith obligations



What is a smart contract

Nick Szabo:

- a set of promises, specified in digital form, including protocols within which the parties perform on these promises.
- technology prevents breaches and substitute enforcement:
 - many kinds of contractual clauses (such as liens, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive (if desired, sometimes prohibitively so) for the breacher
- A crypto-anarcho-capitalist perspective?



Smart contracts: definitions

- **Smart contract**

- a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a [contract](#). Smart contracts allow the performance of credible transactions without third parties. These transactions are trackable and irreversible. (Wikipedia)
- “digital, computable contracts where the performance and enforcement of contractual conditions occur automatically, without the need for human intervention (Wright & de Filippi 2018)
- digital self-executing agreements (Werbach & Cornell 2017)
- "Smart Contracts" are neither smart nor contracts (Nouriel Roubini)
 - They are not smart since they are extremely buggy
 - They are not contracts since no court can enforce them.

Smart contract on Ethereum

- A contract is a collection of code (its functions) and data (its state) that resides at a specific address on the (Ethereum) blockchain.

```
contract HelloWorld { event  
Print(string out); function() {  
Print("Hello, World!"); } }
```

A bit of history: EDI

EDI (electronic data interchange): exchange of standardised document

Machine readable contractual data.

Paper Purchase Order

Purchase Order				
XYZ Company 123 Main Street Fairview, CA 94168		PO Number: 4768 PO Date: 9/30/2012		
Item No.	Quantity	Unit of Measure	Price	Product ID
1	100	EA	27.65	331896-42
Total Items: 1		Total Quantity: 100		

ST*850*540001

BEG*00*SA*4768*65*20120930

N1*SO*XYZ Company

N3*123 Main Street

N4*Fairview*CA*94168

PO1*1*100*EA*27.65**VN*331896-42

CTT*1*100

SE*8*54001

ANSI EDI Purchase Order

UNH+SSDD1+ORDERS:D:03B:UN:EAN008'

BGM+220+4768+9'

DTM+137:20120930:102'

NAD+BY+5412345000176::9++XYZ

Company+123 Main

Street+Fairview+CA+94168+US'

LIN+1+1+331896-42:VN'

QTY+1:100:EA'

PRI+AAA:27.65'

UNS+S'

CNT+2:1'

UNT+10+SSDD1'

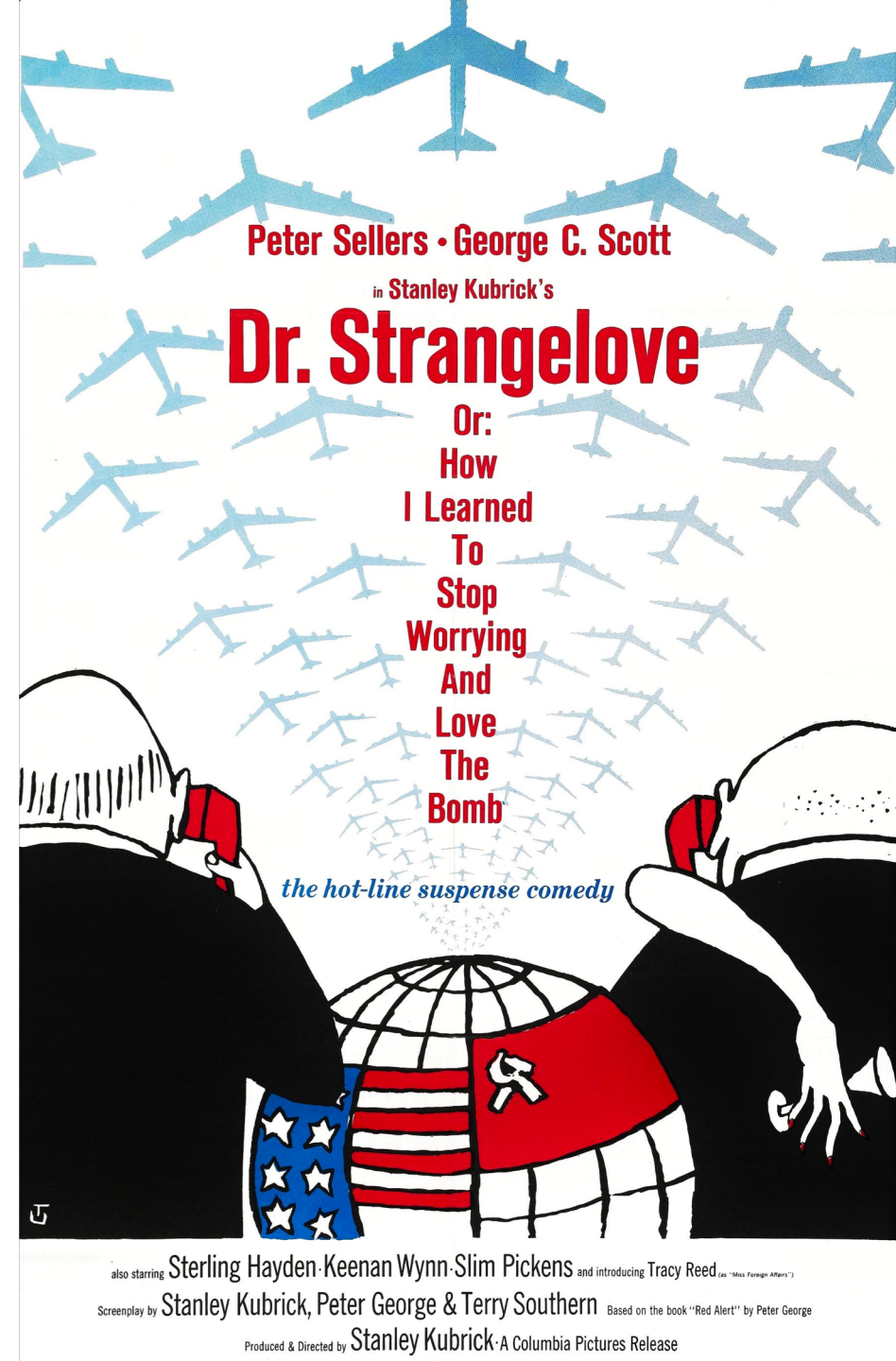
EDIFACT EDI Purchase Order

A bit of history: modelling contract terms in logic / contract agents

- Deontic logic it is obligatory that X, it is permitted that X,
- Action logic: A does X (A sees to it that X)
- It is obligatory/permitted that A does X,
- Rights logic (Hohfeldian concepts): A has the claim that B does X, B has the obligation toward A to do X, A has the power to achieve X, B is subject to A's power
- Condition: under condition C, ...
- Reparation, penalty clauses
- Intelligent agents able to enter into contracts and assess compliance
- Etc.

Smart contracts on the blockchain

- Smart contracts are permanently registered on the blockchain
- They are executed by the infrastructure
- Payments in cryptocurrency
- No need for human intervention
- No possibility to erase the contract
- No possibility to impede further execution (unless foreseen by the contract)









What is an (Ethereum) smart contract?

- An address and a software on the blockchain
- When messages (fund transfers, votes, etc.) are sent to the address, they are processed according to the software (by all nodes of the distributed ledgers)
- The software works autonomously, independently of its creators (unless it contains instructions enabling interference by the creators or third parties on its operations: e.g., to terminate the program, stop some of its functions, etc.)
- The processing redistributes assets (cryptocurrency, tokens, etc.) between the parties

Examples

- An escrow contract between A and B linked to a purchase:
 - A can send money to the contract address
 - A cannot withdraw the money she has sent
 - A can order the money to be forwarded B (e.g. when A receives the merchandise)
- A bet between A and B
 - A and B send the same amount of money to the contract address
 - The money cannot be withdrawn as soon as both amounts have been received
 - If event X happens, the contract sends all the money to A, if X does not happen it sends all the money to B
- Futures
- Crowdsourcing
- Digital autonomous organisations (DAO)
- Insurance
- Stock and bonds
- Purchasing token of physical properties
- Etc.

An empirical analysis of smart contracts on Ethereum.
Bartoletti & Pompianu 2017

Bitcoin	Ethereum	Counterparty
<ul style="list-style-type: none">- Contract blockchain - Public- Language - Bitcoin scripting 	<ul style="list-style-type: none">- Contract blockchain - Public- Language - EVM 	<ul style="list-style-type: none">- Contract blockchain - Public- Language - EVM 
Stellar	Monax	Lisk
<ul style="list-style-type: none">- Contract blockchain - Public- Language - Batch operations + multisignature accounts 	<ul style="list-style-type: none">- Contract blockchain - Private- Language - EVM 	<ul style="list-style-type: none">- Contract blockchain - Private- Language - JavaScript + NodeJS 

An empirical analysis of smart contracts.
Bartoletti & Pompianu

Token	Authorization	Oracle
<p>Distribute some fungible goods (represented by tokens) to users</p> <ul style="list-style-type: none"> - Track the ownership of a physical or digital property (gold, cryptocurrency) - Crowdfunding systems issue tokens in exchange for donations (Congress) - Regulate authorizations and identities, e.g. vote in a poll (ETCSurvey) <p>Standardization proposal in the ERC20</p>	<p>Restrict the execution of code according to the caller address</p> <ul style="list-style-type: none"> - Check if the caller is the owner before performing critical operations - Ensuring that each user vote only once per poll (Corporation) - Define a white-list of addresses that can withdraw funds (CharlyLifeLog) 	<p>The Ethereum language does not allow contracts to query external sites</p> <p>Oracles contracts are the interface between contracts and the <i>outside</i></p> <p>Instead of querying an external service, a contract queries an oracle</p> <p>When the service needs to update its data, it sends a transaction to the oracle</p> <p>The most common oracle is Oraclize</p>
Randomness	Poll	Time constraint
<p>Contract execution must be deterministic: all the nodes must obtain the same value when asking for a random number</p> <ul style="list-style-type: none"> - Query an oracle to generate the value off-chain (Slot) - Generate the number locally, by using values not predictable a priori (Lottery) 	<p>Allow users to vote on some question</p> <p>For instance decide whether an emergency withdrawal is needed (Dice)</p> <p>To determine who can vote and keep track of the votes, polls can</p> <ul style="list-style-type: none"> - Use tokens - Check the voters' addresses 	<p>Specify when an action is permitted</p> <ul style="list-style-type: none"> - In notary contracts, prove that a document is owned from a certain date - Mark different stages of a game (Lottery) - Allow to withdraw funds after a date (BirthdayGift)
Termination	Math	Fork check
<p>Disable a contract when its use has come to an end</p>	<p>Encode the logic which guards the execution of some critical operations</p>	<p>Detect whether a contract is running on the main chain or on the fork</p>

Some issues

- What smart contracts count as “contracts” according to the law ?
- When are they lawful?
- What legal effects do they produce?

Smart contracts and legal contracts

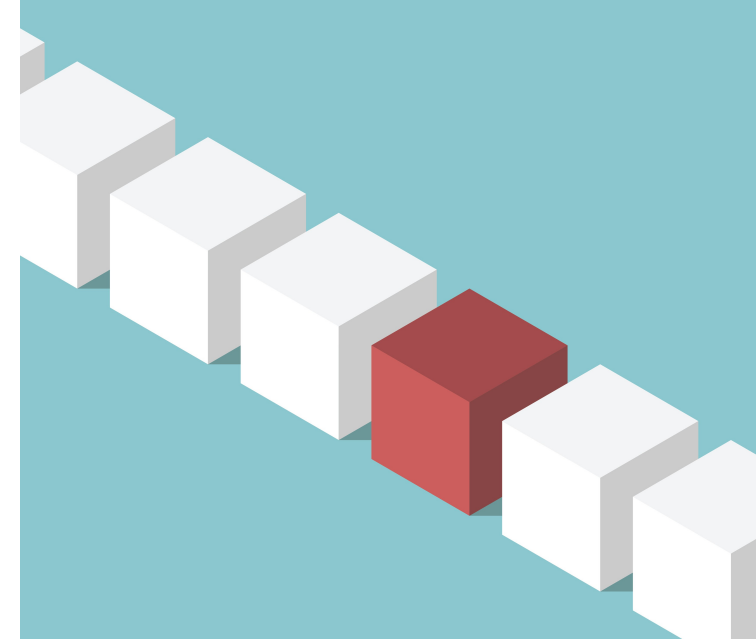
- A smart-contract may not correspond to a legal contract:
 - It may be mechanism that does not implement a transaction between parties
 - It may be a mechanism for a non-binding interaction(e.g., to vote on an initiative that is not legally enforceable)
- A smart contract may correspond to a legal contract
 - It may be a mechanism to perform an off-chain contract already in force (e.g. a cryptocurrency payment to be performed at a certain date)
 - It may be a mechanism that implements and expresses a contract, in some sense: it reallocates digital tokens representing entitlements and so mimics a contract

What is the relation between legal contracts and smart contracts

- The legal contract
 - generates institutional results: it creates, modifies, transfers, rights, obligations and powers (possibly under conditions)
 - Its intended outcome are integrated by the law and subject to judicial review
- The smart contract is a mechanism that creates a computational process over the blockchain.
 - Each parties accepts to trigger the smart contract on the blockchain, where the computational process is created
 - The outcome of the computational process corresponds to results the party has intended or at least accepted.
 - The outcomes are only determined by the software, and subject to no review

What computational processes

- The smart contract introduces further changes on the blockchain,
 - If a result consists in an addition to the ledger (e.g., a payment in cryptocurrency), the smart contract realises the result
 - If a result requires an external computation, the contract can trigger it through a registration on the blockchain, (e.g., block a car for an unpaid instalment)



Smart contracts: opportunities

- Reduce costs for performance
 - Performance is automated (delegated to the contract + the infrastructure)
- Disintermediate
 - Smart contract enable exchange between strangers though trustless coordination (e.g., escrow contracts)
- Provide certainty
 - The result of the contract will be the outcome of the programmed computations

Issues: validity

- A legal contract may be invalid (void or voidable) under various conditions
 - e.g., unlawful content, missing formal requirements, duress, mistake, incapacity of the parties, etc.
- A smart contract
 - may support a transaction that would be legally invalid (e.g. payment for a crime).
 - may include abusive/unlawful contract terms (e.g. excessive interests), which are not valid.
 - may enforce unlawful terms

Problem: how to prevent the creation of invalid contracts, or eliminate their effect. How can the law affect the blockchain?

- Off-chain compensation for damages/reversal

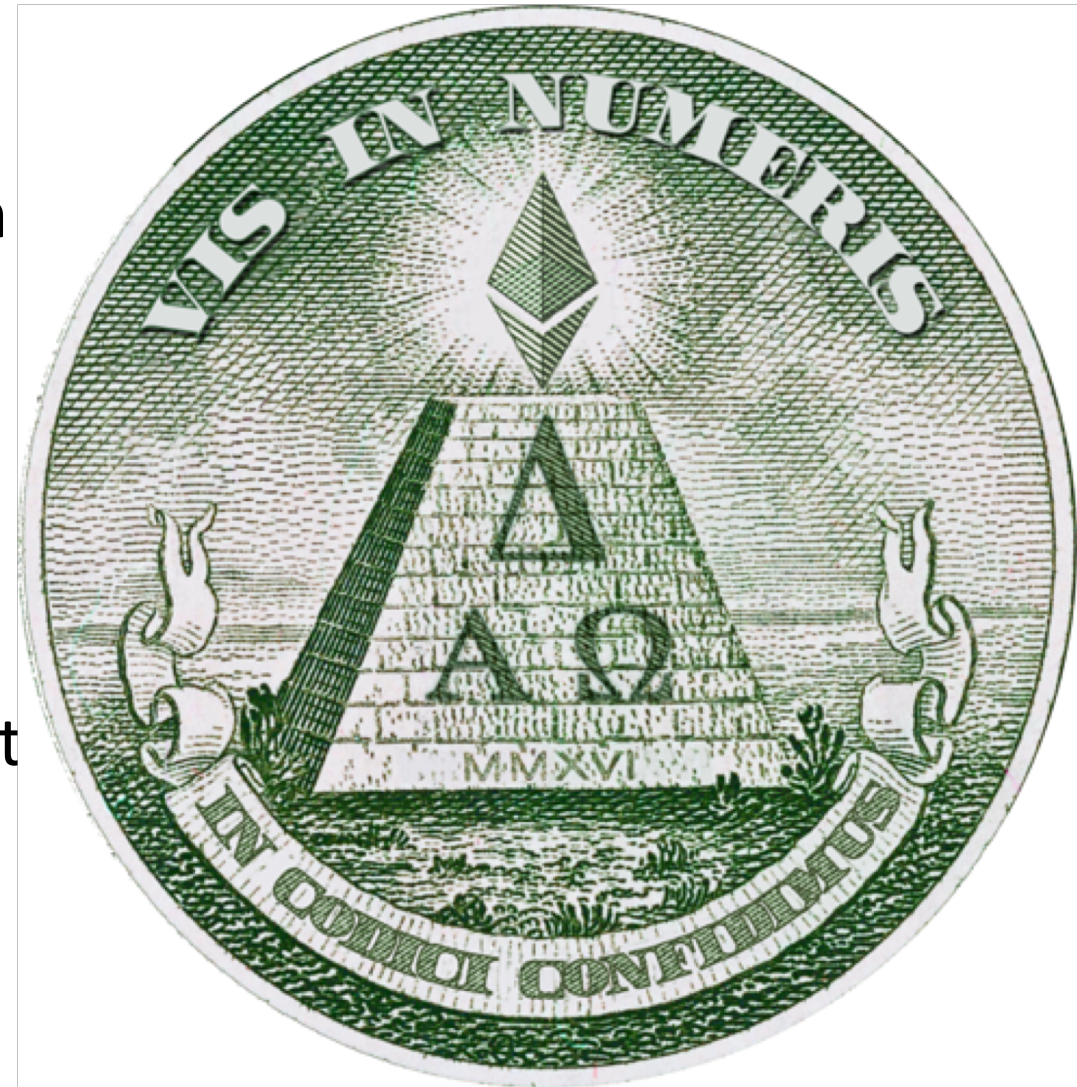
Issue: Interpretation

- A legal contract may need to be interpreted when a doubt arises between the party as concerning the meaning of a term
- Can there be an interpretation issue in a smart contract?
 - What if the execution of the contract is different from what the parties (legitimately) expected?
 - What about bugs in a smart contract?



The DAO case

- The DAO was the largest crowdfunding in history, having raised over \$150m from more than 11,000 enthusiastic member
- An attacker was able to "ask" the smart contract (DAO) to give the Ether back multiple times before the smart contract could update its own balance (so he obtained back multiple time what he sent to the DAO)
- Only way to stop and revert, a hard fork, overriding the code in the blockchain



Issue:

mistakes/deceit/duress/unreasonableness

- What if there the contract contains a mistake, or a party is induced to make the contract through deceit, violence or threat
- What if a computation triggered by the contract appear to be unreasonable (the parties obviously did not foresee it)

Issue: adaptation/relations

- A contract
 - may govern long term relations between the parties, it may need to be adapted to new circumstances
 - A contract may contain open standards
- A smart contract must be sufficiently precise to be automatically processed by the infrastructure
 - Can it refer to a human or AI source to address adaptation/open standards?

Issue: Resolution/termination

- Valid contracts may encounter resolution under various circumstances
 - One party fails to perform obligations
 - One party's performance becomes impossible
 - One party's performance becomes too onerous due to unforeseeable circumstances
- Smart contract in principle cannot be blocked
 - Unless they explicitly include this possibility, maybe conferring this power to an arbiter

Conclusion: great expectations but issues to be solved

- What interface between smart contracts and the legal systems/public regulation
 - Tort law/fraud law/unjustified enrichment against unlawful/abusive contracts (restitution rather than enforcement)
 - Regulation of anonymity/pseudonymity (to address money laundering, criminal activities)
 - Regulation of platforms
 - A new kind of legal remedies?
- New technologies
 - Better languages for modelling contracts
 - Smart-agents (AI) interacting with smart contracts
- How to
 - protect weaker parties
 - enable the achievement of public goals through the regulation of private interactions
 - without breaking the blockchain.

Thanks for your attention

Giovanni Sartor, European University Institute / University of Bologna