LUISS Guido Carli
LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

Dipartimento di **Giurisprudenza**
Cattedra di **Informatica Giuridica**

BLOCKCHAIN TECHNOLOGY AND SMART CONTRACTS:
How can these new technologies be compatible with current Italian contract law?

Relatore
Chiar.mo Prof. Gianluigi Ciacci

Candidato
Andreana De Vecchis
119913

Correlatore
Chiar.mo Prof. Gianfranco Caridi

Anno Accademico 2017/2018

TABLE OF CONTENT

3. Can smart contracts fulfil the formal requirement prescribed for specific contracts by article 1325, (4) Civil Code?

3.a. Relevant European and domestic legislation on electronic documents and e-signatures

3.b. How do smart contracts fit under these pieces of legislation?

4. Smart coding as a suitable tool to express the "economic operation" of contracts

5. Considerations on the recent evolution of the Italian case law on buying orders

CHAPTER 3 - Operative Issues Rising from the Use of Smart Contracts

1. Identity problem on the blockchain

1.a. Pseudonymity, not anonymity

1.b. Decentralised identity solutions

2. General Data Protection Regulation (GDPR) and blockchain technology: an unresolvable conflict?

3. Liability for software breach or bugs on public blockchains

CONCLUSION

BIBLIOGRAPHY

INTRODUCTION

Since the publication of the Bitcoin white paper in 2008, cryptocurrencies have gained increasing attention from the general public, financial sector, academia and national legislators, all attempting to fully grasp the real potential of such a new technological construct and address the challenges it brings with it. Until recently, however, only a few seemed to be aware of the real innovation introduced by Bitcoin: its underlying technology, the "blockchain technology". Indeed, it was only thanks to such a technological foundation that an increasing number of economic transactions have been successfully concluded in what has been defined as a "decentralised" environment, with no central authority being trusted for storing and controlling the transfers of value. The potential of the blockchain has been further developed by the Ethereum Project in 2015, which aimed at providing the technological conditions necessary for the development of so-called "smart contracts", or pieces of code written on the blockchain and embedded with the conditions upon whose realisation the automatic execution of certain transactions arises. The real scope of smart contracts is yet to be discovered, but one thing is certain: given the hype that has been built around the potential of this new technology as a contracting tool, smart contracts are here to stay and legal practitioners will have to get acquainted with them in order to respond to the (many) legal issues they are likely to give rise to.

This dissertation hopes to foster a conversation on such a topic by attempting to provide a definition of the phenomenon and position it within the current legal framework of Italian contract law.

To this purpose, Part 1 will illustrate the ideological underpinnings of the blockchain technology and smart contracting - in the belief that in order to get a deep understanding of these technologies the underlying economic and legal views of those who conceived and developed them should be taken into account -, as well as provide for a technical background of blockchain and smart contracts that will enable the reader to grasp their great innovative reach and will equip him or her with the basic knowledge needed to assess the arguments developed in the following parts.

Part 2 will attempt to respond to the question as to whether or not - and with what adjustments - smart contracts could fit under current Italian contract law. In particular, section 1 of Part 1 will introduce a parallel between traditional contract law - conceived as a centralised, state solution to the problem of trust among distrustful counter-parties in economic relations - and blockchain technology and smart contracting - intended as a decentralised, alternative solution to the same problem. The aim of such a digression is to depict the ambitious scope of blockchain technology and smart contracting, which seem to be challenging state's monopoly over a large range of fields, starting with economic policy and contract law.

Following, Part 2 will critically analyse smart contracts from the perspective of our existing contract law, in the belief that regardless of how revolutionary a technology may seem at the outset, law has proven to be

among the most enduring and resilient human constructs, and its application on new social or technological phenomenons is not a matter of “if”, but rather of “how”. For this reason, the question of how a “meeting of the mind” - an essential element for the conclusion of valid contracts ex article 1325, (1), Civil Code - can be reached through smart contracts is tackled, as well as the question of how smart contracts can meet the formal requirements provided for specific contracts by our national legislation. Furthermore, two additional arguments will be presented to suggest the suitability of smart coding to express valid contractual relations in our legal system: the former will be based on the category of “economic operation” which has risen to interpretative means of contractual clauses; the latter will consider the recent evolution in the Italian case law supporting the theory of the autonomous contractual force of buying orders as a path to the recognition of smart buying orders as a first instance of legally enforceable smart contract in our legal system. Conclusively, Part 3 will outline some of the main operative issues that may arise from the use of smart contracting, namely the identification of contractual parties transacting under pseudonyms on public blockchains, the compliance of blockchain technology services with the new European General Data Protection Regulation, and the liability schemes applicable to public blockchains in cases of software breaches and bugs.

CHAPTER 1

Ideological Underpinnings and Technical Features of Blockchain Technology and Smart Contracts

The origins of the Bitcoin blockchain: the Cypherpunk movement

So far, national states have imposed themselves as the only players in the fields of politics and laws. However, recent technological advancements - most and foremost the blockchain technology - seem to be putting State monopoly over legal matters at risk while questioning the very idea of what the role of the State should be.

This is easily grasped once the philosophical foundations of the 1990 Cypherpunk movement, responsible for both the ideological conception and technical development of the blockchain, are analysed.

The fundamental underpinnings of this movement can be attributed to two apparently opposing forces, working together towards one common goal: the elimination of the State as a legitimate political system in favour of the rise of complete agency of individuals to act at their liberty[1].

Such forces are anarchism on one side[2], leading to the widespread distrust of third parties - governments on top of the list -, and libertarianism on the other, justifying the requirement of a maintenance of agency on individuals through the creation of a money and payment system.

The initial target of the cypherpunks was striking a balance between two fundamentals of the "open society in an electronic age"[3], namely freedom of speech and privacy of personal communication from the public, both considered to be threatened by the increasingly powerful electronic communication technology at the disposal of governments and its potential invasive uses.

Examples of how centralised institutions have abused their tools to interfere with the privacy of online communication have become increasingly prevalent, both at governmental and corporate level. As to the former, in 2011 Wikileaks' "Spy Files" have brought to the general attention the existence of a secret, unregulated mass surveillance industry tracking people's devices and selling the data with States[4]. As to the latter, it is currently under the spotlight the complicated web of relationships that allowed the consulting firm

---

[1] A. Cunningham, *Decentralisation, Distrust and Fear of the Body: the Worrying Rise of Crypto-Law*, Scripted, vol. 13, issue 3, Dec. 2016: https://script-ed.org/wp-content/uploads/2016/12/13-3-cunningham.pdf

[2] T. May, *The Crypto Anarchist Manifesto*, 1988: https://www.activism.net/cypherpunk/crypto-anarchy.html?utm_content=bufferc924a

[3] Eric Hughes, *A Cypherpunk's Manifesto*, 1990: https://www.activism.net/cypherpunk/manifesto.html

[4] WikiLeaks, The Spy Files: https://wikileaks.org/the-spyfiles.html

Cambridge Analytica to have access to the data of millions of Facebook users with an aim to effectively direct its messaging during the political campaign of the current US President Donal Trump[5].

The solution put forward by the cypherpunks was to create anonymous systems allowing individuals to communicate and transact with each other and to do so with coding and cryptography, "with physics and mathematics, not with laws"[6]. The ideological leap flowing from this led one of the main supporters of the cypherpunk credo and inventor of an early cryptocurrency, Wei Dai, to state that in a crypto-anarchy "the government is not temporarily destroyed but permanently forbidden and permanently unnecessary"[7], in his b-money white paper dating back to 1998[8].

These are also the foundations upon which the Bitcoin blockchain described in 2008 Satoshi Nakamoto's white paper[9] was grounded. In blockchain supporters' view, national states and corporations are not acceptable intermediaries and need to be replaced by a technological alternative able to fully realise individuals' sovereignty in free markets, thus circumventing centralised entities like central banks and financial payment networks. Here follows the description of how this is considered to be technically achievable.

1. What is a blockchain?

1.a. Introduction

For the purpose of this analysis, we will define a blockchain as the technological solution to the problem of trust in online economic transactions first introduced by the Bitcoin Whitepaper published by Satoshi Nakamoto in 2008, and further developed by the Ethereum Project since 2015 with the aim to expand its potential in order to create "smart contracts": computer programs encoding contractual clauses that are automatically executed when certain conditions arise.

---

[5] On the Cambridge Analytica ongoing scandal see: https://www.theguardian.com/news/series/cambridge-analytica-files

[6] Quote from John Gilmore's speech on Privacy, Technology and the Open Society, from the First Conference on Computers, Freedom and Privacy, March 28, 1991

[7] Wei Day, b-money white paper, 1998: http://www.weidai.com/bmoney.txt

[8] Here is a more recent statement on the same subject made by software programmer Daniel Larimer in his 2014 interview with Sparks: "I envisage a situation where governments aren't necessary. That the free market will be able to provide all the goods and services to secure your life, liberty and property without having to rely on coercion. That's where this all ultimately leads. The end result is that governments will have less power than free markets. Essentially, the free market will be able to provide justice more effectively and more efficiently than the government can. If you think about it, what is the reason for government? It's a way of reaching global consensus over the theory of right and wrong, global consensus over who's guilty and who's innocent, over who owns what. They're going to be losing legitimacy as more open, transparent systems are able to provide that function without having to rely on force."

[9] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf

Part 1 of this Chapter will attempt to describe the functioning of the Bitcoin blockchain in order to provide the reader with a better understanding of the technical environment within which the creation and execution of smart contracts is made possible, before examining smart contracts in more detail in the second part of this Chapter.

Since its beginning, the Bitcoin blockchain has been processing countless transactions of a digital asset with no backing or intrinsic value and no centralised issuer or controller. This was made possible by the creation of a purely peer-to-peer network which combined for the first time traditional cryptographic protocols and the algorithm consensus known as "proof of work". The result was the creation of a "decentralised ledger" of transactions made available to all the participants on the network and highly safe from external distortions.

Before getting into the details of the functioning of a blockchain, we can get a general picture of it by thinking of a traditional paper or digital ledger and the functions it fulfils: it is a record whose reliability depends on both the intrinsic and extrinsic correctness of its transactions.

In the first sense, we can think of a ledger as the single transactions that make up its pages certifying that two or more parties exchanged X amount of value at a certain time - only those transactions which are deemed to be valid will enter the ledger.

In the second sense, a ledger can also be thought of as the succession of its pages: only if the transactions are listed in the order reflecting their actual succession in time will they be deemed valid in relation to the whole of transactions recorded. As an example, let's imagine a ledger according to which a party, Alice, owns 100€. The transaction through which Alice transfers 80€ to Bob is valid. However, if Alice moves on to transfer 30€ to Eve, this transaction is not extrinsically valid since Alice did not own 10€ she transferred to Eve on the basis of her previous transaction to Bob.

The guarantee of the extrinsic correctness of transactions reached through their correct listing in the succession of pages of the ledger is what prevents parties from "double spending" the same asset, a problem whose solution represented one of the main challenges for the Bitcoin blockchain's developers.[10]

In other words, a ledger will be trustworthy insofar as, simultaneously, each single transaction is valid and is consistent with the rest of the transactions recorded.

In order to fulfil the first requirement (validity of each single transaction) the ledger keeper will be provided with a verification system enabling to univocally identify the parties of the transaction and determine its time and content. As for the second requirement (listing the transaction in the order proving their validity in the light of all the other transactions), the ledger keeper may seal each page, containing a certain number of transactions, so that each change made to that specific sequence of transactions once the page has been sealed reveals that a forge has taken place.

---

[10] For a detailed illustration of the "double spending" problem, see: https://en.bitcoin.it/wiki/Irreversible_Transactions

With this metaphor in mind, we can assume that the first question that blockchain builders had to answer was: how do you create a digital ledger which proves the intrinsic and extrinsic correctness of its transactions? The second question to be responded was: how do you ensure the safety and correctness of such ledger in a system where no central authority takes care of backing the transactions and recording them?

The answers to these questions are provided by what can be considered as the three main structural pillars of a blockchain: (1) cryptographic protocols, in particular asymmetric cryptography and hash functions, which enable the creation of valid transactions; (2) a "peer-to-peer" network of participants of the blockchain, "nodes", connected to each other; and (3) a consensus algorithm know as "proof of work", responsible for recording all the valid transactions in a certain order thus guaranteeing the safety and incorruptibility of the whole system.

1.b. Cryptographic protocols

Cryptography is the practice and study of techniques for secure communication in the presence of third parties: its aim is developing and analysing protocols preventing third parties or the public from reading private messages.

The need for confidentiality in communication has been fulfilled by cryptography since the dawn of culture: an example of this are the rudimental protocols - "cyphers" - used by the Greeks in Classical times. In the modern era, the far more sophisticated system of encryption was developed which translated readable information into codes with no apparent meaning. However, with the rise of the computer era, the scope and use of cryptography has expanded as to guarantee not only the confidentiality of communication, but also its integrity, authentication and non-repudiation through the combined use of disciplines such as mathematics, computer science, electrical engineering, etc. [11]

With this being said, we will define cryptography as the science which translates the analogue tools of signatures, stamps, seals, even identity in a digital form. It does so by using mathematical functions which guarantee computer and information security to a much higher degree than their analogue equivalents.

Both the Bitcoin and the Ethereum blockchain make use of the so-called "asymmetric" cryptography or "public key" cryptography, which enables the creation of digital secrets and unforgeable digital signatures. Each participant on the blockchain is given a pair of digital keys: a private (signing) key and a public (verification) key.

Your private key is a random sequence of numbers produced by the operating system's random number generators using a secure source of randomness or, for those who don't trust the security of such systems, by

[11] B. Mihir, Rogaway, Phillip, "Introduction". *Introduction to Modern Cryptography,* 21 September 2005*,* p. 10.

tossing a coin for a certain number of times until you reach a random private key matching the length and format required by the Bitcoin software.

Your public key is generated by your private key through a one-way, irreversible, cryptographic function: it is easy to calculate your public key from a given private key, but it is computationally infeasible to calculate in the opposite direction, from your public key to your private key.

Once you have your public key you can generate your bitcoin address by applying a "hash" function on it, another one-way cryptographic function which transforms an arbitrary sized input (your public key in this case) into a fixed sized output, referred to as the input's fingerprint or "digest". Bitcoin addresses appear most commonly in a transaction as the recipients of the funds and correspond to the blockchain participants' identity under which they transact (you can think of it as the beneficiary's name on a cheque.)

The field in which public key cryptography has been most widely used is that of digital signatures, which guarantee secrecy and authenticity of digital communications.

Imagine that you want to transfer a digital document to another person and make sure it reaches exactly that person with no forges. You'll have to create a digital signature of that document which is the output of a cryptographic transformation having as its inputs:

- The hash of the document: you will use your arbitrary sized document as the input of a one-way cryptographic function whose output will be a certain fixed sized output, the document's "digest", which would change tremendously if even just a single comma of the document was altered.
- The receiver's public key.
- Your own private key.

The receiver of the digitally signed document will apply a cryptographic function which has as its input the document's digest, the sender's public key and the receiver's private key to verify if the output corresponds to the digital signature. If so:

- The message must have been signed by the owner of the corresponding public key. This proves the authenticity of the document, meaning that it was signed by the sender.
- The message must have been signed with that exact content, since no alterations to its digest happened.
- The message reached exactly the receiver it was supposed to, because only its private key could open it. This guarantees the secrecy of the communication.

Before describing the mechanism through which transactions take place on the blockchain, two preliminary remarks are necessary:

1. Bitcoins - as all the other cryptocurrencies - do not exist anywhere in the world. They don't have any material representation in the form of metal, paper, or any other shape we could come up with if we think

about money as we're used to seeing it. They are nothing but a chain of transactions transferring value from one owner to the next one on the basis of a public ledger to whom every participant has agreed.

2. There is no such thing as a bitcoin balance or account, there are only unspent transaction outputs (UTXO). These can be described as invisible chunks of bitcoins which are transferred on the blockchain through transactions using them as their inputs (where the money is coming from) to create outputs (where the money is going to).

   UTXO can be compared to the currency units of the blockchain: they cannot be divided into smaller pieces, just like you could not think of paying for a £1 water bottle by cutting out one/fifth of a £5 note. They need to be used in their entirety and combined in order to compose an amount equal to or greater than the desired transaction value. In the latter case, you'll have your change back as you would in the example of the £1 water bottle.

   UTXO are scattered around the blockchain, and the only way participants can have an idea of their current balance is by having their wallet application scanning the blockchain to aggregate all the UTXO belonging to them. When a transfer is made to a new owner, a certain amount of UTXO is locked under its bitcoin address which will be redeemed by the receiver by providing for a certain signature - this will be made clear by the description below.

If we think about a blockchain as the digital version of the traditional ledger we mentioned in the Introduction, each line of this digital ledger is represented by a transaction between two parties, that we will refer to as Alice and Bob (of course, transactions can involve more than just two parties but we will use this case scenario for simplicity). In this sense, a transaction on the blockchain can be thought of as a data structure respecting a certain set of rules provided for the by the Bitcoin software and public key cryptography is what enables the creation of transactions while guaranteeing their intrinsic correctness.
Each transaction on the blockchain is made of two parts: an input and an output.
The output of the transaction can be considered as its "payment" part and is made of the amount of value to be transferred (eg. 0,005 btc) and a so-called "encumbrance" or "locking script": the conditions to be met for those funds to be redeemed by the transferrer. In most cases, the encumbrance imposes the requirement for a digital signature, meaning that the funds will be unlocked only by the private key corresponding to the public key used by the transferor to encrypt the transaction.
In the case of Alice's transfer to Bob, she will include a script in the output of her transaction saying something like: "This output is payable to whoever presents a signature from the key corresponding to Bob's public address."
The output of a transaction can be considered as the destination of the value that is being transferred, from Alice to Bob, and it represents Alice's debit against Bob and Bob's credit against Alice.

According to remark number (2) we know that value can be transferred on the blockchain on the basis of the UTXO owned by the transferor, which must be used in their entirety and combined to amount to the desired transaction value. For this reason, it may happen that the the transferor wants to transfer as the output of her transaction less btc than the total UTXO she owns. If this is the case, she will have to include a second output in her transaction where she pays herself back the "change" resulting from the difference of UTXO she is sending minus the output she intends to transfer to Bob. This transaction is automatically included in the output by the transferor's wallet, which will also take care of reserving a certain part of this change to the miner who will successfully include Alice's transaction in the blockchain as a "transaction fee".
Such fees work as an economic incentive for miners to promptly and correctly validate transactions in the blockchain, as it will be further explained in the paragraph 1.e on "Economic Incentive".
Transaction fees are not mandatory and transactions with no fees may be successfully recorded on the blockchain. However, since fees affect the processing priority of transactions, including one which is appropriate to the "weight" of the transaction (meaning the amount of computational effort it takes to record it on the blockchain) ensures that the transaction will be promptly processed and included in the ledger.
The input part of the transaction is made of the so-called "transaction hash" and "unlocking script": the former points to the previous transaction(s) containing the UTXO that are being spent in the output, the latter unlocks those funds by solving the "encumbrance" that the transferor of those UTXO in the previous transaction put on it. By solving the encumbrance (providing for the digital signature required) the transferrer of those funds proves its ownership and control over them and is now allowed to transact them.
The input of a transaction can be considered as the origin of the value that is being transferred, from a certain previous transferor to Alice, and it represents Alice's credit against that transferor which she is now transferring to Bob.
There is an exception to the input/output chain just described which is represented by the so-called "coin-based" or "generation" transaction opening each new block. This transaction is included by the miner who successfully mined the block and included it in the blockchain and creates brand-new bitcoins payable to that miner as a reward for mining. This is the system through which the bitcoin's money supply is created during the mining process and it will be further described in the paragraph 1.e on "Economic Incentive".
In the light of this, we can define an electronic (bitcoins or ether) as a chain of digital signatures or of digitally-signed declarations by one party (the transferor, Alice) of her intent to transfer a certain amount of value to another party (the transferrer, Bob), on the basis of a record of previous transactions to which everybody has agreed in which the transferor, Alice, was identified as the recipient of previous transfers of that value.

Conclusively, it is worth stressing out that cryptographic protocols provide such a high level of security that even if it is theoretically possible to break cryptographic-secure systems, it is infeasible to do so by any known practical means[12].

As a consequence, the system of transactions taking place on the Bitcoin blockchain - and the more complex transactions implemented by the Ethereum blockchain - are backed by a degree of reliability far higher than that provided for by the analog or digital schemes currently used to guarantee the safety of transfers of value and legal relations in general outside the blockchain.

1.c. Peer-to-Peer network

The structure and creation of a bitcoin transaction has been described so far. However, this represents only one of the phases of a transaction's lifecycle which is concluded when it has been accepted as valid by all the participants on the network ("nodes"), included into the ledger as its permanent part, and confirmed by sufficient subsequent blocks of transactions. Only at this point, will the transferrer, Bob, be able to unlock the output of Alice's transaction to him and exercise its right of disposal of the asset by turning it into the input of his new transactions to different transferrers, following the same rules and procedure as the transaction that Alice made in his favour.

By doing this, the chain of transfers of value which constitutes the ontological essence of cryptocurrencies as described by point 1 of the previous paragraph is created.

To this purpose, each digitally-signed transaction will have to be broadcasted to the rest of the so-called "peer-to-peer" network, which will be responsible for its verification and inclusion in the shared ledger.

In fact, each bitcoin node is connected to a few other nodes discovered during startup through the peer-to-peer protocol. Once a transaction has been created, it will be publicly transmitted to the connected nodes who will independently validate it according to a set of rules described by the Bitcoin software before propagating it any further to their connected peers.

On the basis of the independent validation procedure carried out by the first receiving node, the transaction will either be deemed to be valid and forwarded to the rest of the network, or invalid, in which case the transaction will be rejected by the receiving node who will send it back to the originator, with the result that malformed transactions will not go beyond one node.

This validation procedure of transactions does not require the intervention of any intermediate entity: the blockchain's functioning is enabled by a self-sufficient network which is responsible - and rewarded, as will be discussed below - for the security of system.

---

[12] See note 2

1.d. De-centralised consensus algorithm: "Proof-of-Work"

The real innovation introduced by Satoshi Nakamoto in the 2008 Bitcoin Whitepaper is the process through which global consensus is achieved in a network with no central authority.

The main feature of such decentralised consensus is that it does not result from an election made by the nodes - since no ordinary voting processes are used - nor does it happen at a fixed moment of time. Instead, it is an "emergent consensus"[13]: "an artefact of the asynchronous interaction of thousands of independent nodes, all following simple rules".

The human element in the creation of such consensus has been completely nullified by the introduction of a new objective parameter: the computation power required to create "blocks" of transactions to forward to the rest of the network for verification and confirmation.

Before illustrating the process through which decentralised consensus is reached and the role of computation power to this end, it will be useful to go back to the metaphor of the analog ledger we started off with and think of the blocks of a blockchain as its sealed pages, whose succession guarantees the extrinsic correctness of transactions, meaning their validity in relation to the whole of transactions that took place. Only valid transactions listed in a way that is consistent with the other transactions recorded will be confirmed by the network and become part of the blockchain's immutable history.

The process through which such consensus is achieved starts with the collection of verified transactions into "blocks" by specialised nodes called "miners". Their job is to create a perfect block of transactions which respects a set list of criteria and solves the so-called "Proof-of-work". To do so, miners are required to solve an extremely complex cryptographic puzzle (which will be briefly described below). The solution to the puzzle can only be found by brute force: expensive hardwares specialised exclusively on the processing of complex cryptographic functions will be put to work until such solution is found, with the consequence that an incredible amount of computation power needs to be used with related high electricity costs.

The proof-of-work carried out by miners is what creates trust in the blockchain: only those blocks proving that a certain amount of computational effort has been put into their mining will be accepted as valid.

This consensus algorithm requires miners to scan for a value ("nonce") that results in a block hash that is less then the "difficulty target".

To understand this, let's imagine each block of the blockchain as composed of two parts: a header and the list of transactions. The block header is hashed to obtain the block's unique and unambiguous digital fingerprint, which identifies it in the blockchain.

Each block header contains, among other things: a "previous block hash" field and a so-called "nonce". The former contains the unique digital fingerprint of the last block created on the blockchain and its inclusion in

---

[13] Andreas M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, 2014

the subsequent block header implies that the smallest change to a block will result in a change of its digital fingerprint, which requires a change in the subsequent block referring to it in its "previous block hash" field. This creates a chain of generations of blocks whose modification is only possible if all the computation required to reach that point of the blockchain is carried out again.

For this reason, each block in a blockchain could be compared to a layer of a geological formation: the most superficial layers may be blown away by the wind, but as time passes their presence will be made permanent with the deeper layers telling a story that cannot be changed.

The "nonce" is the value that miners need to find to come up with a hash of the block which respects the so-called "difficulty target". You can think of the difficulty target by picturing a dice game where players throw the dices repeatedly trying to throw less than a specific target. If this target is 12, unless you throw double-six, you win and you won't need many throws to do it. As the target decreases, the probability of a winning throw decreases and you'll need more and more throws before getting a winning throw. The difficulty target is the threshold value that a block hash must respect to be considered valid.

Only by committing huge amount of computing power (implying expensive hardware and electricity costs), miners will be able to find the nonce and solve the PoW.

This system has the important corollary that Satoshi explains as follow: "Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it"[14], thus decreasing the chances of a malevolent attack being able to corrupt the blockchain.

The first miner to solve the proof-of-work will propagate the new block to the network for verification. Once verified, the creation of a new block will start with more and more layers piling up on top of each other. This results in the creation of a chain whose authoritativeness is represented by the amount of computing power required to mine it.

1.e. Economic incentive

Each new block starts with the "coin-based transaction", mentioned in paragraph 1.b. With it, the "winning" miner awards himself a certain amount of bitcoin as a reward for successfully doing the proof of work. The sum of all the transaction fees of the block is added to the coin-based transaction thus increasing the reward for the miner.

Transaction fees will become the sole form of incentive once the predetermined amount of 21 million BTC is put into circulation by 2140.

[14] Satoshi Nakamoto, note 10

The main functions of the coin-based transaction are: (1) creating the bitcoin's money supply, thus compensating the lack of a central authority doing so; and (2) providing for an economic incentive for nodes to support the network.

Conclusively, it is worth stressing that the blockchain establishes a reward system which encourages nodes to stay honest on the basis of the simple assumption that playing by the rules will always be more profitable than breaking them. As Satoshi puts it: "If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth."

The safety and incorruptibly of the system is not in the hands of one or more entities to trust, but rather trust is achieved by means of cryptographic protocols to be respected in order to be economically rewarded. In other words, a blockchain creates a system within which playing by the rules pays off, whereas cheating is expensive and counterproductive.

The combination of the cryptographic, game theory and economic element typical of the blockchain functioning coined the term "crypto-economics" to refer to this type of system.

The rise of the Ethereum blockchain: Decentralise everything!

Once the technological foundations of the blockchain were laid down by Bitcoin, the scope of the so-called "ancap" (anarcho-capitalist) revolution soon went beyond the private exchange of messages and transfer of value, and set out to allow contract negotiation and business conduction in a completely decentralised, allegedly secure and anonymous fashion, with parties not ever knowing their legal identities[15]. Thanks to the invention of the Ethereum Blockchain in 2015 by then nineteen-year old Vitalik Buterin, there was an important shift in the potential application of this technology: from a decentralised digital cash system, the blockchain now carries the promise of providing for a decentralised execution environment of agreements. In fact, as Buterin explains in the Ethereum White Paper, the Bitcoin blockchain represents a "tool of distributed consensus" which can be improved in order to implement "more complex applications having digital assets being directly controlled by a piece of code implementing arbitrary rules: "smart contracts"[16]. The problem of trust minimisation in economic transactions solved by the Bitcoin blockchain has expanded as to include the need of parties to enter agreements with the guarantee that "no matter with which other individuals, systems or organisations they interact, they can do so with absolute confidence in the possible outcomes and how those outcomes might come about"[17] - to use the words of Ethereum co-founder Gavin Wood.

The mission of the Ethereum Project is to provide for a solution to this need which has been identified in the creation of a Turing-complete[18] blockchain where users can establish rules and conditions of agreements to be automatically executed by the blockchain itself.

However, the idea that technologies could be used as a legal tool with the aim of regulating users' behaviour dates back to the early days of the Internet [19] in the same way as the concept of automatically executable contracts was first described - and the term "smart contract" coined - by computer programming and law graduate Nick Szabo in his 1996 article "Smart Contracts: Building Blocks for Digital Markets"[20].

---

[15] See note 11

[16] Vitalik Buterin, *Ethereum White Paper: A Next Generation Smart Contract & Decentralised Application Platform*, http://www.the-blockchain.com/docs/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

[17] Gavin Wood, *Ethereum: A Secure Decentralised Generalised Transaction Ledger*, https://bravenewcoin.com/assets/Whitepapers/Ethereum-A-Secure-Decentralised-Generalised-Transaction-Ledger-Yellow-Paper.pdf

[18] Turing-completeness refers to the ability of a machine to perform any possibile calculation or computer program, given an appropriate algorithm and the necessary time and memory

[19] See Lawrence Lessig, *Code, and Other Laws of Cyberspace,* 1999, where the author coins the famous expression "code is law"

[20] Nick Szabo, *Smart Contracts: Building Blocks for Digital Markets,* 1996: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

Nonetheless, it was only with the Ethereum blockchain that the technological background for their practical realisation was provided.

The real scope and application of this new form of agreement has not been clearly defined yet. Opposing opinions have arisen, with the most convinced supporters of the technology claiming it will cause the role of lawyers to be completely downsized - if not completely nullified - in many areas of contract law[21], next to the more placid position of those considering them not "smart" not "contracts"[22].

The discussion that follows aims at providing a clear definition of the term "smart contracts" and illustrating some use cases. It will do this in the belief that traditional and smart contracts can coexist in a way that is mutually beneficial and in the attempt to outline how this can happen.

2. What are smart contracts?

The term "smart contract" is being increasingly used by blockchain developers, law professionals and the general public as a comprehensive concept within which, however, distinctions need to be drawn in order to fully grasp its scope and attempt to address the challenges it raises.

The purpose of this section is outlining the different meanings that are being attributed to the term "smart contract" before narrowing the list down to a definition which is pertinent to the legal analysis of the phenomenon which will be further developed in the following chapters.

It will be useful to start this discussion clarifying what smart contracts are not by comparing them to a few existing forms of contracts mistakable with smart contracts.

First of all, smart contracts are not electronic contracts. In fact, electronic contracts are written agreements in digital form whose substance and execution are subject to the application of law by courts just as their paper counterparts.

Such "paperless" contracts can be stipulated either by means of digital and electronic signatures - most commonly used within online business-to-business relations in order to safeguard the integrity and non-repudiation of the contract - or take the form of so-called "clickwrap" agreements typical of online business-to-consumer relations where the need for bargaining celerity is paramount, so much so that consumers can currently enter agreements by skipping the long text of the terms and conditions and just clicking on the highlighted boxes at the bottom of the agreement.

Developments in the field of computer programming language triggered the evolution of electronic contracts into more sophisticated forms of agreement with a higher degree of involvement of computing in the

---

[21] Alexander Savelyev, *Contract Law 2.0: «Smart» Contracts As the Beginning of the End of Classic Contract Law*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885241

[22] Gary J. Ross, *Why Lawyers Won't Be Replaced By Smart Contracts*, https://abovethelaw.com/2017/10/why-lawyers-wont-be-replaced-by-smart-contracts/

definition of contractual clauses and assessment of their compliance, namely "data-oriented" and "computable" contracts described by Harry Surden in his 2012 article "Computable contracts"[23].

"Data-oriented" contracts are the translation of substantive contractual obligations from natural legal language into "structured data", a highly defined format which can be readily processed by computers. The advantage of "data-oriented" contracts is enabling the comparison and computational analysis of legal obligations in a way that is not feasible through written-language documents.

Once a computer is able to read contractual terms, it can be provided with information about the meaning of such terms agreed by the parties and data about the world to "make automated, prima-facie assessments of conformance" with those terms.

These "computable" contracts are widely used in the financial sector and the most common use case are "computable option contracts", which confer the right to buy a predetermined amount of asset at a certain price within a fixed expiration date. Once the option contract is translated into structured data with a clear expiration date and a certain price, the computer can be linked to an agreed source of information about the price of the asset and automatically assess compliance with the contracts once the price reached the one agreed in the terms, or deny compliance of any transactions attempting to buy the asset at a date subsequent to the expiration date provided.

The main limitation of computable contracts is that their prima-facie assessment does not enable the automatic execution of the agreement itself. Moreover, were the parties unsatisfied with the results of the computable contract, they could still act before a traditional court which would disregard those results.

Even though a higher level of machine autonomy is reached through the use of the above-mentioned contracts, they can all be considered as expressions of the process of digitalisation of economic and business relations whose aim has been delivering the same objective as their traditional versions faster.

As Co-director of the Imperial College Centre for Cryptocurrency Research Dr. Catherine Mulligan explains: "Previous generation of technologies were responsible for faster and more secure exchange of information. Blockchain, meanwhile, is about the exchange of value; it is intended to enable individuals to exchange currency and other assets with one another without relying on a third party to manage the contracts and transactions".

Electronic, data-oriented and computable contracts still represent what Nick Szabo describes as "wet code": "rules and conditions having a verbal source and translated into text on paper or computers to be interpreted by the human brain"[24].

---

[23] Harry Surden, *Computable Contracts*, University of California, Davis, 2012: https://lawreview.law.ucdavis.edu/issues/46/2/Articles/46-2_Surden.pdf

[24] Nick Szabo, *On The Blockchain and Smart Contracts*, : https://www.youtube.com/watch?v=tWuN2R2DC6c

Smart contracts, on the other hand, are expressions of "dry code": their rules and conditions are set, verified, executed and interpreted by machines or softwares with no need of human intervention - by allowing the automatic execution of agreements, they have the potential to entirely redefine the framework within which economic and legal relations take place.

Once the external perimeter of the notion of smart contracts has been outlined by distinction with some widely-used types of contracts, an analysis of its internal classification is necessary in order to provide a clear definition of "smart contract" on which the following chapters are based.

Such analysis will be carried out by illustrating the different meaning of the terms: (1) smart code; (2) smart legal contract and (3) smart alternative contract.

2.a. Smart code

The widely-spread and indiscriminate use of the term "smart contract" is misleading insofar as it is centred around the traditional notion of "contract", without making any reference to what is to be considered as the real innovation behind such tool: smart coding.

While the first blockchains such as Bitcoin were designed to perform a small, well-defined amount of relatively simple operations - namely, the transfer of currency-like tokens - the purpose of the Ethereum blockchain is to be a platform for smart codes, thus enabling the creation, storage, verification and execution of any pieces of code.

If intended in this sense, smart codes are sophisticated softwares living on the blockchain and sharing unique features compared to their "off-chain" versions.

Firstly, they are recorded on the blockchain, which gives them the characteristic permanence and censorship resistance described in paragraph 1.d.

Secondly, they are automatically executed by the blockchain itself when the conditions set up in the code are verified.

Smart codes are being improved in order to allow the collection and verification of real-world information to be submitted to the blockchain, thus enabling the inclusion of off-chain conditions into the code.

In fact, we can think of smart codes as agents living in the "walled garden" of the blockchain and being unable to fetch external data on their own[25].

To solve this problem, parties to smart codes agree upon so-called "oracles", the procedure which is deemed responsible for providing external data to the blockchain and triggering the execution of the code. Smart codes may need different types of information, provided by different types of oracles.

[25] http://www.oraclize.it/

To make a few examples, smart option contracts are dependent upon the asset having reached a certain price fixed by the parties, and the execution of the option contract requires the smart code have a reliable data-source of the price of the asset. In this case, "software oracles" handling information available online can be implemented into the smart code so that the price of the asset is defined on the basis of a website indicated by the parties (Bloomberg, etc.) and the option is executed once the asset reaches the price fixed by the parties.

Moreover, the execution of smart insurance contracts is dependent upon the occurrence of a certain event (a fire, or the client's death, etc.). In this case, the parties agree upon a "hardware oracle" to be implemented into the smart code which will carry information directly from the physical world. The function of hardware oracles can be fulfilled by either a single entity external to the blockchain - which raises the question of trust to the entity itself - or a decentralised network whose nodes are called to back and certify the occurrence of certain events through their digital signatures[26].

The third essential characteristic of smart codes, arguably the one responsible for their disruptive potential, is that they have direct control over blockchain assets through control over their corresponding cryptographic key.

Although cryptocurrencies are the main asset currently stored and transacted on the blockchain, more complex "real life" assets are being brought "on-chain" within a process of digitisation aiming at allowing their registration and transaction in the forms and with the advantages offered by the distributed ledger technology.

Examples of real life assets being brought on-chain are provided by the projects currently developed in the field of land and intellectual property registers.

Traditional land registers have proven to be expensive - so much so that the Australian government of New South West has sold management rights on its land register to a hedge fund[27] - unreliable - we can make the extreme example of Haiti, where all paper records were destroyed by the 2010 earthquake, or consider the more common scenario of illegitimate copies or manipulation of paper or digital records - and inefficient, due to the time and costs of recovery efforts.

To solve these problems, real estate properties' records can be transformed into digital representations by means of hashing functions and cryptographic keys to be uploaded on the blockchain, considered the only technological solution currently available able to guarantee their long-term, authentic conservation[28].

---

[26] For a brief overview of the function and issues related to oracles, see: https://cointelegraph.com/explained/blockchain-oracles-explained

[27] http://www.abc.net.au/news/2017-04-12/$2.6-billion-price-tag-on-nsw-land-titles-registry-sale/8439176

[28] https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf

Georgia has been the first country to pioneer a blockchain-based land title project, with about 100.000 properties already registered on the blockchain[29].

Intellectual property registers are also likely to become one of the main applications of the blockchain technology.

While the acquisition of rights related to trademarks and patents is subject to their registration, in our national legal system copyright is unregistered and comes into existence automatically at the moment of creation of an original creative work, with the consequence that it may be hard for authors to prove ownership of their work and for third parties to know who to seek licenses from.

In addition to this, the ease with which creative works can be uploaded, shared and transformed on the Internet makes it even harder for authors to claim their rights and effectively exercise them.

By uploading original creative works on the blockchain, not only can authors obtain immutable evidence of their ownership at the moment of creation - comparable to a digital certificate of authenticity - , but they will also be able to track the complete chain of transfers of their work on the Internet, see where and how it is being used and seek licenses from users.

Once it is clear that real life assets can be translated into cryptographic keys, uploaded, stored and transacted on the blockchain, it is easier to understand the reason for the inclusion of the term "contract" in relation to what has to be considered merely as a sophisticated piece of code: it enables the transfer of value on the basis of the conditions agreed upon by the subjects involved in the transfer and programmed into the smart code itself.

The analogies of Vitalik Buterin are a helpful tool in the attempt to further characterise smart codes, which he describes as "cryptographic "boxes" that contain value that only unlocks if certain conditions are met", while clarifying that they "should not be seen as something that should be "fulfilled" or "complied with"; rather, they are more like "autonomous agents" that live inside of the Ethereum execution environment, always executing a specific piece of code when "poked" by a message or transaction, and having direct control over their own ether balance"[30].

When these three features of smart codes are cumulatively considered, one can grasp the disruptive potential of this new tool. Here follows a brief illustration of some of the possible implementations of smart coding in relation to the above-mentioned fields of real estate and intellectual property rights.

As to the former, the Swedish Land Register is currently working on a project aiming to launch an app where real estate transfers can happen within a matter of seconds. By storing and making available real estates'

---

[29] https://eurasianet.org/s/georgia-authorities-use-blockchain-technology-for-developing-land-registry

[30] See note 8

records on a private/permissioned blockchain[31], parties such as buyers, sellers and banks can interact through digital identification and signatures to make purchase offers, enquiry about credit loans and have them accepted by the bank, even sign the bill of sale, which will result in a considerable reduction of the time and costs of purchase and sales agreements[32].

As to blockchain implementation in relation to copyright, authors will be able to set up the conditions for the diffusion of their works on the Internet. They could require that a micropayment is made to their crypto account by any users willing to download, share or transform their work, with the result that they could directly monetise their economic rights without the need for any of the big intermediary companies currently taking a share on them (like Youtube, Netflix, etc.). In this light, smart coding could be considered as an innovative and effective tool of Digital Right Management (DRM).

On the basis of these simple use cases of smart coding, the reason for inclusion of the term “contract” in relation to what is merely a piece of code becomes clearer: smart contract codes refer to smart codes whose “object" - to use a term borrowed from our traditional contract law - has economic value (e.g. money or assets with economic value, such as property or IP rights, etc.), which would justify the creation of a traditional binding contract to ensure that the parties be able to enforce the terms[33].

However, smart codes need not resemble anything we would ordinarily think of as a “contract”. In fact, next to applications in relation to financial transactions (which represent the best-suited and currently most developed field of implementation of smart coding[34]), smart coding could become a killer-app in the field of e-voting[35] and corporate governance schemes[36], to name but a few.

---

[31] In unpermissioned blockchain networks, nodes can restrict participation by appointing a group of participants who are given the express authority to provide the validation of blocks of transaction or participate in the consensus mechanism. An analysis of the differences between permissioned/unpermissioned or private/public blockchains is beyond the scope of this paper, but for an illustration of benefits, security and trust issues of permissioned blockchain networks see: https://monax.io/explainers/permissioned_blockchains/

[32] See note 18

[33] Josh Stark, *Making Sense Of Blockchain Smart Contracts*, 2016: https://www.coindesk.com/making-sense-smart-contracts/

[34] For a summary on the potential impact, benefits and risks of the use of smart contracts in the financial sector, see: https://www.capgemini.com/consulting/wp-content/uploads/sites/30/2017/07/smart-contracts.pdf

[35] Scientific Foresight Unit (STOA) of EPRS, European Union, *What If Blockchain Technology Revolutionised Voting?*, 2016: http://www.europarl.europa.eu/RegData/etudes/ATAG/2016/581918/EPRS_ATA%282016%29581918_EN.pdf

[36] David Yerman, *Corporate Governance and Blockchain Technology*, NYU Stern School of Business, 2016: https://corpgov.law.harvard.edu/2016/01/06/corporate-governance-and-blockchains/

2.b. Smart legal contract

In his 1996 paper, Nick Szabo coined the term "smart contract" and provided for a straightforward definition of the concept as "a set of promises, specified in digital form, including protocols within which the parties perform on these promises"[37]

For the purpose of this analysis, and following the discussion developed in the previous paragraph on the nature and functioning of smart coding, we will further characterise "smart legal contracts" as specific use cases of smart coding replacing or complementing existing legal contracts through the articulation, verification, execution and enforcement of agreements without the need of human intervention[38].

In the discussion that follows, the term "smart contract" will be used to refer to the notion of "smart legal contract" provided, which stays separate from the concept of "smart code" of par. 2.a.

An attempt to position such a technologically advanced form of agreement into the Italian traditional contract law framework will be provided in Chapter 2.

This paragraph will provide a brief overview of some of the key features of smart legal contracts and their benefits when compared to their traditional counterparts, before illustrating a spectrum of possible forms they can take with a view to start addressing some of the issues relating to their use as contracting tools.

Smart legal contracts share the same features described in relation to smart codes, namely (1) they have digital form and (2) are embedded, meaning that contractual clauses are implemented in softwares as code. Additionally, (3) their execution is mediated by the blockchain technology which gives them (4) irrevocability so that, once initiated, the outcomes for which a smart legal contract is encoded to perform cannot be stopped unless there are unmet conditions.

From these traits one can deduce that smart legal contracts are necessarily deterministic in nature: all possible outcomes of the agreement (including penalties for breach of contract) must be explicitly stipulated in advance[39].

The elements of the deterministic nature and irrevocability raise the challenging question of how to deal with modification of terms in and anticipated termination of smart contracts.

We will focus the attention on how to prevent hypothesis of impossibility of the contract due to a change in the legal landscape (nullità sopravvenuta per norme sopraggiunte dopo la conclusione del contratto) and how to allow anticipated termination (risoluzione) of smart contracts, by analysing these two contractual occurrences on the basis of the Italian contract law.

---

[37] Nick Szabo, see note 20

[38] See note 23

[39] Primavera De Filippi, *Legal Framework For Crypto-Ledger Transactions*: https://wiki.p2pfoundation.net/Legal_Framework_For_Crypto-Ledger_Transactions

As to the former, we can imagine the case of a smart loan agreement where the interest rate agreed upon by the parties turns out to illegal on the basis of the new threshold model imposed by an act of the Italian Bank subsequent to the creation of the smart loan. There must be ways to guarantee compliance of smart contacts such as this to the evolving legal system and one method would require the backing of the State through the creation of a publicly available database and application programming interface (API) of relevant legal provisions, which would be related to the terms of the contract by being embedded into the smart code. By doing this, smart contracts would be able to update their provisions' terms in accord with the national database[40].

The implementation of this method could result in the State's API having a master override over smart contract terms, which would represent a case of legal limitation of the principle of freedom of contract ex art. 1322 c.c.

An alternative method is purely private and has the benefit of not having to rely on the third-party State to create a new infrastructure: ex post policing on the compliance of the smart contract to the evolving legal system can be put on the parties, who have the burden to update the code accordingly.

As to ways to allow the anticipated termination (risoluzione) of smart contracts, we can picture the inclusion of both termination event clauses (condizioni risolutive) and unilateral termination clauses (recesso convenzionale) in the smart code.

As in traditional legal contracts, the actualisation of the termination event encoded in a smart contract would result in the automatic termination of the contract relationship, with the difference that the verification of such actualisation in smart contracts would be entrusted to oracles - which would result in enhanced certainty as to the moment of occurrence.

The codification of unilateral termination clauses (recesso convenzionale ex art. 1373, c.c.) into smart contracts is also possible, and their enforcement could be subject to the previous payment of the agreed compensation (multa penitenziale) in favour of the other party, which would happen automatically once the unilateral termination clause is activated. Furthermore, did parties agree upon the inclusion of the temporal limitation to the exercise of the unilateral termination faculty provided by art. 1373, cc., smart coding would simplify compliance to such requirement by voiding the unilateral termination clause as soon as execution of the contract occurs.

With this being said, it is evident how codification of traditional contractual terms requires the translation of natural legal prose or legalese into automatically executable performances by smart codes which, in turn, results in the minimisation or sheer absence of textual ambiguity in smart contracts. This is seen as a pivotal

---

[40] Max Raskin, *The Law and Legality of Smart Contracts*, Georgetown Law and Technology Review 305, 2017: https://www.georgetownlawtechreview.org/the-law-and-legality-of-smart-contracts/GLTR-04-2017/

trait of smart contracting compared to traditional legal contracts, and its operative implementation is currently at the core of influential academic and technological research such as that illustrated by Clack, Bakshi and Braine in their paper "Smart Contract Template"[41] and carried out by the open source data-model CommonAccord[42], whose aim is to enable the automatic drafting of legal documents through the diffusion of a global template of codified legal texts.

When talking about smart contracting, a clarification on the forms that smart contracts can take is essential in order to outline if and how they can interact with traditional legal contracts and prevent legal difficulties. A wide spectrum of formal possibilities is available, where one extreme is represented by the "code is contract" school of thought holding that smart codes can completely replace natural legal language by embedding the entirety of contractual clauses into running programs.

The main critique to such a daring statement is that the current state of codification of contractual clauses has not yet reached the level of sophistication required to develop fully-fledged smart contracts, and general legal clauses - such as "material adverse change", "reasonable steps", etc. - still represent an unescapable element of "wet" code typical of contractual relations whose meaning has to be determined by legal analysis. Although it may be argued that future developments in the field of codified legal text are likely to start a trend towards the clarification of or reduction in the use of such general clauses, difficulties in relying exclusively on smart codes as the only record of parties' rights and obligations would still arise, as in the case of smart contracts deemed to not have legally binding effect by a court which would then have to settle the contractual relation.

On the other end of the formal spectrum, smart contracts are downsized to mere digital tools of performance of contractual relations - such as payments - while the creation and regulation of agreements is still entrusted to traditional legal contracts. The risk carried by this conservative approach is that of preventing that the full potential of smart contracting will ever be reached and limiting the benefits that this tool could bring to contractual relations.

There is a range of intermediate possibilities which are more in line with the codification technology available and better-suited to face the legal difficulties brought by smart coding. In fact, smart contracts could be duplicated with separate natural legal documentation in paper or electronic form where each clause encoded into the smart code has its matching natural legal version, and viceversa. However, the preferred solution by both technological developers and legal practitioners seems to be that of "split" contracts, ripping the gains of automation by encoding non-human performances into computer code, while including

---

[41] Clack, Bakshi, Braine, *Smart Contract Templates: foundations, design landscape and research directions*, 2016: https://arxiv.org/pdf/1608.00771.pdf

[42] On CommonAccord, see: http://www.commonaccord.org/

wider human obligations, remedial and other provisions into written legal prose, with the two components making a cohesive contract[43].

The use of split contracts has been described as a way to create an effective and mutually beneficial interaction of smart coding and traditional contract law, allowing the smart contract to remain simple in the execution of contractual performances while relying on the legal contract to handle edge cases arising at the enforcement level[44].

Not only would split contracts compensate for the current lack of technological tools for complete codification of contractual terms and provide a solution to difficulties arising from the implementation of smart contracts, but they would also enable the use of smart contracting to regulate relations for which formal legal requirements are provided by the legal system, ad substantiam or ad probationem.

2.c. Smart alternative contract

To conclude this part on the definition of smart contract and related concepts, reference must be made to so-called smart alternative contracts.

The development of increasingly more sophisticated computers, applications and machines has opened the way to a whole new type of commerce, and commercial agreements, that happen instantaneously between those entities. Examples of machine-to-machine commerce of this kind are smart cars having control over their account and paying to recharge themselves at charging stations, or washers that buy their own detergent with no need of human intervention.

These transactions still require a minimum level of trust to be commercially viable, but are ill-suited for traditional legal contracts which are comparatively expensive and require the involvement of legal persons (humans or corporations).

Smart coding is the perfect match for this new type of commerce, and has been implemented to create novel, alternative forms of agreements.

---

[43] R3 and Norton Rose Fullbright white paper, *Can smart contracts be legally binding contracts?,* November 2016: http://www.nortonrosefulbright.com/files/r3-and-norton-rose-fulbright-white-paper-full-report-144581.pdf

[44] See note 30

Final remarks

For many, the blockchain technology carries the same - if not more - revolutionary potential as the Internet. However, strong criticism has understandably been levied against the cypherpunks and blockchain supporters in general, whose extremism has got them the epithet of "technological utopians". Some commentators focus on their "dissociative anti-government" motif - aiming at turning citizens into active partners of a government perceived as too slow, corrupt and elitist - to object that the notion of State cannot be referred to as a distant third party, but should instead carry with it the immanent and complex social and historical process rooted into our Constitutions "that makes us us"[45]. Others question the capability and opportunity of an algorithm-based global society to carry out essential political processes such as the resolution of conflicts or the adjustment of social iniquities. It is beyond the purpose of this essay to enquire whether an algorithm-based governance capable of replacing governments is technically achievable and socially desirable. Nonetheless, one cannot help but drawing a parallel between the uncompromising individualism and anti-statism of both the blockchain and early Internet's supporters[46]. In fact, the Internet was also seen as the key to permanently undermine national regulation through decentralisation and enhanced citizen's agency, but that was before governments figured out how to impose their authority and will on the Internet, which in some cases turned into one of states' preferred tool for citizens' monitoring and repression[47]. Blockchain may share the same faith and its supporters be deeply disappointed by the bending of the technology to the needs of centralised institutions, as it is already happening, with giant financial institutions and national governments launching their own private blockchain to increase productivity[48].
The hope is that rather than demonising each other's ideological foundations and technical solutions, both centralised institutions and decentralisation supporters will realise that a positive collaboration is needed in order to reap the greatest benefits of both systems.
As far as the legal field is concerned, the first step towards such a positive collaboration lies in gaining a deeper understanding of what smart legal contracts are and how they could be positioned within our legal system, which is precisely the aim of the next Chapter.

---

[45] M. Atzori, *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?,* December 1, 2015, Available at SSRN: https://ssrn.com/abstract=2709713 or http://dx.doi.org/10.2139/ssrn.2709713

[46] K. Werbach, *Trust, But Verify: Why the Blockchain Needs the Law,* August 1, 2017, Berkeley Technology Law Journal, Forthcoming. Available at SSRN: https://ssrn.com/abstract=2844409 or http://dx.doi.org/10.2139/ssrn.2844409

[47] Evgeny Morozov, *The Net Delusion*, 2011

[48] For a critical analysis on the risks of a concentration of blockchain-based solutions in the hands of centralised authorities: I. Bogost, *Cryptocurrency Might be a Path to Authoritarianism*, May, 2017, The Atlantic: https://www.theatlantic.com/technology/archive/2017/05/blockchain-of-command/528543/

CHAPTER 2

An analysis of the positioning of smart contracts in the Italian traditional contract law system

Introduction

This Part will enquire about the legal status of smart contracts in the view of establishing whether they could be considered legally binding agreements under Italian contract law.

It will do this by developing a multi-level analysis of the phenomenon from a general theory of contract law, legislative and jurisprudential standpoint.

First, traditional contract law will be described as a centralised solution to the problem of lack of trust between counter-parties in economic relations, to then move on to illustrate how the Bitcoin blockchain technology claims to offer, for the first time in history, an alternative, decentralised solution to the same problem with reference to transfers of value, and how the Ethereum blockchain claims to expand such a solution to any transfer of rights and obligations through smart contracts.

The second section of this Part will present smart contracts as the technological and juridical evolution of "virtual contracts", in order to outline similarities and differences between these two tools with an aim to draw some conclusions relating to the status of the parties and pre-contractual phase of smart contracts, as well as describe how the essential requirement of a "meeting of the mind" prescribed by article 1325, (1), Civil Code can be validly reached in smart contracts.

Section 3 of this Part will describe the current state of the European and Italian law on electronic documents, e-signature and e-commerce and the strong technical features that such instruments share with smart contracts, with an aim to suggest that the principles, definitions and solutions developed with regards to the former could be extended to the latter, and that smart contracts could be deemed to fulfil the formal requirements provided for specific contracts by article 1325, (4), Civil Code.

Section 4 will illustrate the category of "economic operation" which spawned from the reframing of the notion of contractual "cause" ex article 1325, (2), Civil Code, and its relevance as an interpretative device of contractual clauses, with an aim to support the suitability of smart contracting to clearly and effectively regulate contractual relations.

Ultimately, section 3 of this Part will recall the recent evolution in the case law of the Italian Civil Supreme Court on buying orders which has abandoned the interpretation according to which these should be considered as mere executions of the framework brokerage contract, in favour of the recognition of their autonomous legally binding force, thus introducing a third, jurisprudential basis to the opportunity of attributing contractual force to smart contracts.

1.a. Traditional contract law as a centralised solution to the problem of trust among distrustful counter-parties

One of the foundations of the contemporary economic and social world lies in the ability of parties who did not know nor trust one another, to transfer value and rights through mutually binding promises - that is, to transact - on the basis of their recognition of and reliance upon a higher power responsible for the backing of such promises - that is, the state.

The description of such mechanism has been at the core of legal theories, one of which was developed by the XVII century English philosopher Thomas Hobbes.

In Hobbes' view, famously outlined in his 1651 "The Leviathan", in the real or hypothetical absence of any state sovereignty - the so-called "state of nature"[49] - human beings would experience a condition of permanent war of "every man, against every man" condemning them to a "solitary, poor, nasty, brutish and short" life[50]. In this scenario, without notions of right and wrong, justice and injustice, where "force, and fraud, are in war the cardinal virtues"[51], Hobbes claims that it is only through the rational appreciation of their need to secure self-preservation against death, that men can elevate themselves and access a civil state[52], in which a "social contract" is stipulated between the subjects and a single sovereign entity (the Leviathan), on the basis of which the former give up their individual rights on the use of force in favour of the latter.

Here lie the foundations of the concept of state monopoly of the legitimate use of physical force - later postulated by sociologist Max Weber in his famous essay "Politics as a Vocation"[53] -, which still holds out as one of the defining features of modern national states exercising it through their arms of police and military forces.

Understandably, in the state of nature the creation and execution of valid agreements is strongly jeopardised, if not altogether impossible. As Hobbes himself put it:

---

[49] André Munro, *State of Nature, Political Theory*, Encyclopaedia Britannica: https://www.britannica.com/topic/state-of-nature-political-theory

[50] Thomas Hobbes, *The Leviathan*, 1660, Chapter 12: https://www.ttu.ee/public/m/mart-murdvee/EconPsy/6/Hobbes_Thomas_1660_The_Leviathan.pdf

[51] Ibid

[52] Ian Ward, *Thomas Hobbes and the Nature of Contract*, Studia Leibnitiana, Bd. 25, H. 1 (1993), p. 96: https://www.jstor.org/stable/40694231?refreqid=excelsior%3Ab0add425d732263ce7d75799356642a6&seq=7#page_scan_tab_contents

[53] M. Weber, *Politics as a Vocation*, 1919: "A state is a human community that (successfully) claims the monopoly of the legitimate use of physical force within a given territory".

"**If a covenant be made**, wherein neither of the parties perform presently, but trust one another; **in the condition of mere nature, (which is a condition of war of every man against every man,) upon any reasonable suspicion, it is void**: but if there be a common power set over them both, with right and force sufficient to compel performance, it is not void. For he that performeth first, has no assurance the other will perform after; because the bonds of words are too weak to bridle men's ambition, avarice, anger, and other passions, without the fear of some coercive power; which in the condition of mere nature, where all men are equal, and judges of the justness of their own fears, cannot possibly be supposed. And therefore he which performeth first, does but betray himself to his enemy; contrary to the right (he can never abandon) of defending his life, and means of living.
But in a civil state, where there a power set up to constrain those that would otherwise violate their faith . . . he which by the covenant is to perform first, is obliged so to do"[54].

Consistently, the solution formulated by Hobbes lies in the recognition of a central entity entitled to intervene to enforce agreements in cases of breach:

"(…) **There must be some coercive power, to compel men equally to the performance of their covenants, by the terror of some punishment, greater than the benefit they expect by the breach of their covenant**; and to make good that propriety, which by mutual contract men acquire, in recompense of the universal right they abandon: and such power there is none before the erection of a commonwealth (…)"[55].

"(…) So that **the nature of justice consisteth in keeping of valid covenants**; but the validity of covenants begins not but with the constitution of a civil power sufficient to compel men to keep them"[56].

[54] See Hobbes, 14.18

[55] See Hobbes, 15.13

[56] See Hobbes, 15.15

In Hobbes' theory, the problem of lack of trust[57] between counter-parties is remedied by demanding them to put their trust in the hands of a third neutral party, placed above all of them and legitimised by the recognition of its presence as necessary for the safety of the people[58].

Since Hobbes, the trend towards the creation of centralised organisations enabling economic interactions of distrustful parties through top-down coordination and hierarchical structures has not been significantly altered[59].

Still nowadays, national governments - or supranational organisations legitimised by them[60] - monopolise currency supply, and their control over any transfer of money is exercised either directly, by public financial institutions, or indirectly by private financial institutions, which are nonetheless authorised and regulated by provisions of public law[61].

If one goes beyond the sole transfer of money to consider any types of patrimonial relationship, the centralised nature of the system designed to ensure the enforcement of contracts is even more blatant: bailiffs, judges and courts are the resources allocated by national civil judicial systems to ensure performance of contractual obligations.

In this view, traditional contract law can be seen as the centralised solution elaborated by the state to solve the problem of lack of trust among counter-parties by shaping a system of incentives and deterrents on the basis of which they find it more convenient to play by the rules than breaching them[62].

---

[57] Please note that this essay is not concerned with the concept of "trust" formulated by Roman contract law (*fideicommissum),* nor with the Common law typical institution of the same name. Instead, the term "trust" is used here to refer to the social relation of "expectation that arises within a community of regular, honest, and cooperative behaviour, based on commonly shared norms, on the part of other members of that community", as defined by political economist Francis Fukuyama in his *Trust: Social Virtues and the Creation of Prosperity,* Simon and Schuster, 1996, p. 26

[58] Isaak I. Dore, *Deconstructing and Reconstructing Hobbes*, Louisiana Law Review, vol. 72, num. 4, 2012, p.842 : https://digitalcommons.law.lsu.edu/cgi/viewcontent.cgi?article=3070&context=lalrev

[59] M. Atzori, see note 45

[60] As it is the case for the European Member States belonging to the Eurosystem, within which the European Central Bank administers the monetary policy on the basis of the Treaty on the European Union (Treaty of Maastricht)

[61] For an updated overview of the regulation of the activity of private financial institutions in the Italian legal system, see: Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica, emanated by the Italian Central Bank and entered into force on June, 1st, 2016: http://www.gazzettaufficiale.it/eli/id/2016/06/01/16A04096/sg

[62] Josh Stark, *The Two Topics in Law and the Blockchain,* 2016: https://www.coindesk.com/the-two-topics-in-law-blockchain/

This function is fulfilled by regulating contractual relations at the ex-ante and ex-post level. From the former flows the definition of traditional contract law as the "branch of the law which determines the circumstances in which a promise shall be legally binding on the person making it"[63], in regards to the activity of the national legal system of settling the formal and substantial requirements which turn a mere promise into a legally binding contract[64].

The ex-post or remedial nature of traditional contract law, on the other hand, is evidenced by the of definition a contract as "a promise or a set of promises for the breach of which the law gives a remedy"[65], thus alluding to the regulation of a system of remedies at the disposal of counter-parties once the relationship of mutual trust is broken.

By operating on these two levels, traditional contract law draws the perimeter within which contractual parties can exercise their freedom to contract, while providing some degree of legal protection both to the counter-parties' interests throughout the course of their contractual relation and to those of the public.

1.b. Blockchain technology and smart contracts as an alternative decentralised solution to the problem of trust among distrustful counter-parties

For the first time in history, recent technological advancements open up the path to a viable alternative solution to the problem of trust, thus challenging the well-established assertion of the necessity of a trusted third party (financial institutions or national legal systems) acting as the sole efficient and reliable guardian of economic relations.

Here follows a brief analysis of how the Bitcoin blockchain elaborated such a solution with reference to the transfer of value in electronic transactions and how the Ethereum blockchain expanded it to any contractual relationships through the creation of smart contracts.

In this author's opinion, such analysis is a necessary preliminary to assessing the question of whether or not smart contracts could be deemed to be valid contracts under Italian contract law. In fact, only once it is clear what the scope and potentiality of the blockchain technology is, it is possible to fully grasp the advantages brought by smart contracts in the field of contract law and realise that there is no fundamental reason why they should not be recognised as legally binding agreements.

---

[63] A.G. Guest, *Anson's Law of Contract*, Twenty-sixth edition

[64] On this note, see Francesca Fasullo, *Il Principio di Autonomia Privata e Contrattuale*, according to whom: "L'autonomia contrattuale è dedotta dall'ordinamento giuridico, in quanto si forma su uno strumento già predisposto dal legislatore, quale è il contratto"

[65] The American Restatement (Second) of the Law of Contracts, 1981, Ch. 1, art.1: https://www.nylitigationfirm.com/files/restat.pdf

At the very beginning of the Bitcoin White paper, it is made clear that the creation of an electronic payment system with no central authority entrusted with issuing coins and processing payments was essential to overcome "the inherent weaknesses of the trust-based model" [66] monopolised by financial institutions. According to the white paper, reversible transactions, mediation costs increasing transaction costs, impossibility for micro-payments are just a few of the downsizes of such model[67], which need to be bypassed by "allowing any two willing parties to transact directly with each other without the need for a trusted third party"[68]. It is worth mentioning how here, the tendency towards increased individual agency at the expense of central authority described in Part 1 as one of the foundations of the blockchain phenomenon emerges, and will be recalled later on in this section when the theory of contracts as individual economic programs is presented.

Contrarily to physical money, however, it is not easy to prevent people from spending digital cash twice through replication, falsification or by taking advantage of the few minutes it takes for transactions to be fully processed on the blockchain, which gives rise to the so-called "double spending problem", representing a crucial passage in both the logical and technical process outlined by Satoshi Nakamoto.

The cruciality of such problem should not be measured exclusively against the disruptiveness of the technological solution developed to solve it - the blockchain technology -, but rather, and more importantly for the purpose of this analysis, it lies in the fact that it carries with it proof that even those moved by the strongest aversion towards traditional trust-based models, like Satoshi, realise the unavoidable need to create some mechanism to address the fundamental issue of trust once they confront themselves with any form of social interactions - even if electronic -, which contradicts the criticism raised by those commentators according to whom trust on systems like Bitcoin or Ethereum is felt as unnecessary[69]. As a matter of fact, the blockchain technology does not dismantle the concept of trust nor liquidates it as unneeded, but rather, it reframes it by introducing a practicable substitute to centralisation.

The initial proposal of a "mint", or trusted central authority issuing new coins and checking transactions to avoid double spending was soon discarded by Satoshi, and understandably so, since in imitating the functioning of a bank, it tainted the system with the very same vice it aimed to erase.

---

[66] Satoshi Nakamoto, see note 9

[67] Ibid

[68] Ibid

[69] A. Cunningham, see note 1

An alternative solution was put forward: cryptographically secure transactions are made publicly available in a system in which each participant is required to agree on a single history of order on the basis of an algorithmic-based consensus, Proof-of-Work.

The functioning of the Bitcoin blockchain and the description of how it creates decentralisation was covered in Part 1, to which reference is made. Here suffices it to stress that the "computationalism"[70] introduced by the Bitcoin blockchain translates the problem of trust from trust into something or somebody into a "trustless trust"[71], in which the universal languages of mathematics, cryptography and coding replace the need of human intervention in the enforcement of transactions, and in which the openness, transparency and (presumed) incorruptibility[72] of decentralised systems nullify the need of a central authority supervising the correctness of transactions and having the exclusive power to intervene in cases of breach.

The "civil power" that Hobbes deemed necessary "to compel men equally to the performance of their covenants, by the terror of some punishment, greater than the benefit they expect by the breach of their covenant", now seems to have a different face: from a single authority, the state, monopolising the use of force to ensure enforcement of agreements, it may now be conceived as a more efficient and decentralised system designed to ensure the same exact purpose without relying on force[73].

As already mentioned, the scope of such a blockchain-based trust model has soon been broadened.

The incorporation of a Turing-complete programming language by the Ethereum project in 2015 has enabled the embedding of autonomous software agents on top of the blockchain, so-called smart contracts, with the ability to automatically execute more complex transactions than those happening on the Bitcoin blockchain. The technical features, current and potential applications of smart contracts have already been illustrated in Part 1, to which reference is made. Here suffices it to say that just as before blockchain, the tool of traditional contract law has been used to codify agreements and render them enforceable by a central authority (the state or "Leviathan), under the new paradigm schematised in the chart below, smart contracts may be seen as the tool used to codify agreements and render them enforceable by the blockchain.

---

[70] See A. Cunningham, p. 244: "computationalism" is described as "complete faith in the ability of mathematics and technology to eradicate problems emerging from human behaviour"

[71] See note 11

[72] Such incorruptibility is not absolute, since bugs in the system are possible and can be taken advantage of from malevolent users, as it was the case in the now infamous "DAO hack" of 2016. Part 3 of this essay will focus on the question of liability in cases of bugs in the system resulting in a damage to participants of the network.

[73] See note 11

Solution to the problem of lack of trust among distrustful counter-parties

	Centralised solution:	Decentralised solution:
Entity enforcing agreements	State	Blockchain
Tool for contracting	Traditional contract law	Smart contracts

Expectedly, strong criticism has been levied against the notion of trust adopted by blockchain developers and the role of law that flows from it.

As to the former, some commentators have labeled Nakamoto's expectations regarding trust as too ambitious, since they aim at the complete elimination of risk among transacting parties, which is instead regarded as an immanent element of the notion of trust itself ("Without the element of risk, there is no trust")[74].

As to the latter, it has been observed how law, rather than technology, is to be considered the most adequate tool to regulate human interactions since it is concerned with aligning the imperfections of our human nature in a way that is beneficial to the parties involved in matters of justice and to the public interest, and does this by depending and relying upon the human element "that one accused of a crime or injustice would hope to appeal to"[75].

However, it should be noticed that raising criticism towards the blockchain technology on the basis of the assertion that risk is an immanent element of trust and accusing its developers of unrealism for attempting to reduce or eliminate such risk overlooks the fact that when technology enables to overcome what may be seen as immanent and unavoidable traits of the human condition (like risk in relations of trust) it should be embraced rather than being made object of suspicion.

Similarly, objecting that cryptography and computationalism in general cannot actually realise absolutely unbreakable trust neglects that when technology provides more satisfying solutions to human problems, it should be empowered, even if such solutions cannot be deemed perfect.

This is not intended to foster a position of blind faith towards the potential of the blockchain technology. It would be naif to believe that math and cryptography alone have the ability to solve once and for all the problem of trust in human interactions. In fact, subjective intent remains relevant even when expressed through objective code, making blockchains vulnerable to the same types of selfish

[74] See Cunningham, p. 244

[75] See Cunningham, p. 255

human behaviours it intends to solve, like hacker attacks, fraud and manipulation[76]. For this reason, it is embraceable the position of those scholars pushing for a cooperative interaction between blockchain developers and legal scholars, where the former recognise the relevance of well-established governance principles developed by the latter throughout their century-long experience, and the latter are willing to adapt their formal structures and institutions to let technology come to aid where it is needed and beneficial to the legal system[77].

With regards to the objection that law as an imperfect science is the best-suited tool to regulate human interactions, while this author agrees that appealing to human reasoning skills may be preferable than relying on the dry, positivistic approach of algorithms in criminal matters[78], a distinction should be drawn with reference to contract law matters, to which the clarity, unambiguity and determinism of code language could be of great potential benefit[79], as will be further illustrated below.

Conclusively, the blockchain offers a diverging view on the role of trust in human interactions and a very different mechanism to achieve it.

Public actors and law practitioners should not just record such fundamental difference and, on that basis, commit the error of discrediting the benefits that the application of the blockchain technology is likely to bring to the legal field.

Rather than establishing an unsolvable dichotomy between centralised and decentralised trust models, it is advisable that a middle way is found where legal professionals, on one side, are willing to open up to the opportunity of introducing technological tools to their toolbox which will remedy the current inefficiencies of the legal system, and technological developers, on the other side, recognise the contribution of legal experts as essential for the positive development of technological solutions[80].

---

[76] K. Werbach, *Trust, But Verify*, Berkeley Technology Law Journal, p. 7: https://poseidon01.ssrn.com/delivery.php?ID=130069006013112001115065122069013031034018053020030049097003099125124109002069082122020018034045018032097090102026115125106065044016056009084004123100001025099100037023032116031026067004079085125069075076088004110121109066107080018083010086068078117&EXT=pdf

[77] Ibid. For a description of mutually-beneficial cooperation models between code and law, see pp. 48-58

[78] L. Dormhel, *Why Your Next Judge (Probably) Won't Be A Robot?*, December, 2013: https://www.fastcompany.com/3015563/why-your-next-judge-probably-wont-be-a-robot

[79] A. Wright and P. De Filippi, *Decentralized Blockchain and the rise of Lex Cryptographia*, Mar, 2015, p. 24: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664

[80] For an analysis of three possible mechanisms of cooperation between "dry" and "wet" code, meaning the blockchain technology and legal systems, see Werbach, pp. 23-30

2. Can smart contracts meet the essential requirements prescribed by article 1325, Civil Code for traditional contracts?

In order to assess whether the formation and execution of legally binding agreements can validly arise from auto-executing pieces of code embedded on the blockchain, it is essential to determine whether and how the foundational elements of a contract required by our traditional contract law (art. 1325, Civil Code. Indicazione dei requisiti) can be transposed into the code itself.

The first requirement for a promise to turn into a legally binding contract ex art. 1325, Civil Code is the reaching of a "meeting of the mind", or mutual assent ("accordo"), between the contractual parties, together with the presence of a lawful "cause", a determined or determinable "object" and a specific form, if so required either for the validity of the contract itself (ab substantiam), or for evidence of the contract's existence and of each party's consent in legal proceedings (ad probatiotem). Additional formalities for the validity of certain contractual clauses may be prescribed according to the informative duties lying on certain contractual parties in favour of the other (so-called "informative formalities"[81]).

This part will enquire on the procedures of formation of a "meeting of the mind" between contractual parties transacting through a smart code. Given the heterogeneity of the relations that can potentially be settled through smart codes, it will be useful to start by providing the widest possible legal framing of the phenomenon which considers the common features of all types of smart codes, and to do so by referring to existing models and definitions elaborated by our doctrine as a consequence of the disruptive rise of electronic contracts and e-commerce in the last decade.

2.a. Smart contracts as the technological and juridical evolution of "virtual contracts": similarities and differences

Smart codes may be considered as the technological and juridical evolution of "virtual contracts"[82]. With this term, scholars refer to a *species* of the "telematic contract" *genus*. While the latter comprises any contractual agreements reached through the use of a telecommunication channel, such as phone, fax, telegrams, emails, etc.[83], "virtual contracts" are characterised by an additional feature: they are reached through telecommunication services deploying the Internet as their essential technological foundation, which then

---

[81] Here reference is made to the existing national regulation on restrictive/unfair clauses codified by articles 1341-1342, Civil Code and by articles 33-38, 141-142, D. Lgs n. 206/2005 (Consumer Code). While the former piece of legislation applies to cases of standard, mass contracts with unilaterally predisposed clauses concluded between private parties, the latter applies to each single business-to-consumer (B2C) contract.

[82] The notion of "virtual contract" was first introduced by E. Tosi, in his *Contratto virtuale. Procedimenti formativi e forme tra tipicità e atipicità*, Milano, 2005

[83] E. Tosi, *Diritto privato dell'informatica e di Internet, I beni - I contratti - Le responsabilità*, Milano, 2006, 131 ss.

becomes the tool used by the contractual parties to express their contractual will, form contracts and (in some instances) execute them.

Virtual contracts, however, are not all the same. *Senso latu*, any agreement reached through an exchange of e-mails or any other Internet-stored telecommunication service falls under the definition of virtual contract. *Stricto sensu*, virtual contracts make the narrower category of agreements reached on web pages where contractual offers are unilaterally predisposed by the offeror to the general public of the offerees, or Internet users, who are free to accept the offer and conclude the contract through the "point and click" procedure or a typical telematic form of contract formation[84].

Smart contracts may be considered as the technological and juridical evolution of virtual contracts, in that they share the need of the Internet as their technological basis to express and form the agreement, but have peculiar features that virtual contracts as we currently know them lack:

1. Smart contracts need a blockchain to exist and be embedded on: visually, the Internet could be pictured as the technological foundation for any virtual contracts, on which the additional layer of a distributed ledger technology must be added to allow for the creation of a completely virtual transacting space;
2. Smart contracts grant automatic execution of contractual clauses: their automatic execution is not a possibility, but rather, one of the distinguishing features of coding as a transacting tool.

From the characterisation of smart contracts as virtual contracts one important corollary follows: the principle of auto responsibility elaborated with reference to the parties' contractual conduct on the Internet shall be extended to the use of smart coding too, given that the use of the blockchain technology requires the Internet as its technological basis.

According to principle of auto responsibility online, Internet users who freely access the virtual market and conclude "point-and-click" contracts do so under their responsibility based on a presumption of their

84 The "point-and-click" procedure is the most widespread form of manifestation of consent to the conclusion of e-contracts that are not subjected to any formal requirements: once the forms on the vendor's website have been filled in by the offeree, by clicking on the "agree", "buy" or "chart" button, the online contractual offer is accepted, an electronic notice is sent to the vendor and an e-contract is concluded. Such a procedure is considered to be an "atypical" telematic form of contract formation, which can lawfully be prescribed by the online vendor on the basis of the provision of article 1326, (4), c.c., according to which offerors are free to unilaterally select the form in which the offeree's consent shall be manifested (when there are no legally-prescribed formalities). Next to the point-and-click procedure, there are "typical" telematic forms of contract formation represented by qualified and digital signatures, whose definitions and effects are clearly outlined by European and domestic legislation.

knowledge of the full meaning and effects of the telematic language, regardless of wether they are actually familiar with such a language in the specific cases[85].

Given the ease with which "point-and-click" contracts can be concluded and legal obligations arise from them, it shouldn't sound as an overstatement that blockchain users transacting through smart coding would theoretically be covered by a higher level of protection against "IT risk" than they currently are under the principle of auto responsibility on online transactions. As a matter of fact, transacting through smart codes requires the fulfilment of a preliminary procedure made of specific steps: users need to set up their wallet by purchasing the cryptocurrencies which will provide for their transacting funds, and they can do so by either accessing an online exchange service and making a wire transfer from their bank account or card, or they can take part in the Initial Coin Offering[86] of new tokens - which will then be used to transact on the specific platform which is launching the token itself - by either transferring cryptocurrencies from their wallet or making fiat payments. Only once these steps are successfully undertaken, will an Internet user become a blockchain user with a public and private key to transact with. For this reason, it is to unlikely that someone unawarely enter a smart code, since the predisposition of the technological background required to do it can be seen as a manifestation of a user's intention to start transacting on the blockchain.

A parallel could be drawn between getting a public and private key to transact on the blockchain with and getting a credit or debit card from a bank: in the same way as the lawful single transactions concluded by the card owner would be deemed valid on the basis of the initial card agreement concluded with the issuer (which, of course, excludes cases of card theft or fraud), the single smart contracts regularly entered into by blockchain users could be deemed valid on the grounds that they manifested their assent to transact on the blockchain when they set up their wallet.

---

[85] See E. Tosi, *Il contratto virtuale: ricostruzione della categoria negoziale,* in *I contratti informatici,* curated by R. Clarizia, in Rescigno, Gabrielli, *Trattato dei contratti,* Milano, 2007: "L'enunciazione dell'assunzione del *rischio informatico* per effetto del *principio di autoresponsabilità*, consente, quindi, con riferimento al codice iconico del linguaggio telematico, di prospettare agevolmente, nella contrattazione telematica, una *presunzione di conoscenza* della semantica telematica che il contraente telematico - edotto o meno del linguaggio in parola - si accolla nel momento in cui decide liberamente di accedere al mercato virtuale".

[86] An Initial Coin Offering (ICO) is a type of crowdfunding used by cryptocurrency start up companies to raise capital by selling their newly issued "tokens" to investors and supporters of the project in exchange for legal tender or other cryptocurrencies such as bitcoin or ether. Being an unregulated capital-raising process, ICOs enable blockchain start ups to bypass the regulated, rigorous and expensive investment channels provided for by venture capitalists and banks. ICOs represent one the most successful examples of smart contracts currently run on the blockchain, with 435 successful projects and $5.6 billion raised in 2017 (See Grut, *Only 48% of ICOs were successful last year - but startups still managed to raise $5.6 billion*, in Business Insider UK: http://uk.businessinsider.com/how-much-raised-icos-2017-tokendata-2017-2018-1?IR=T). They got the attention of national regulators by the end of 2017, when the People's Bank of China officially banned them, citing them as disruptive to economic and financial stability. Another major hit was suffered by the technology when Facebook banned ICOs advertisements stating that many of them were "not currently operating in good faith", and Twitter, Google and Bing followed.

When considered as a more advanced version of virtual contracts, however, smart contracts show some unique features which distinguish them from the former.

As a matter of fact, the heterogeneous types of virtual contracts have been pooled in together by our doctrine on the basis of distinguishing traits relating to the status of their parties (business, consumers or public administration) - from which specific formalities may arise -, their pre-contractual phase and the procedure for contract formation. It will be useful to briefly outline such features with an aim to characterise smart codes as a separate contracting tool and draw some conclusions relating to the status of their parties, their pre-contractual phase and the procedure for their formation.

The first consideration is on the status of the parties of stricto sensu virtual contracts: considering the investment in terms of hardware and software required to establish online contractual relations, most of the parties offering their goods and services online are businesses, which makes the Internet as the preferred contracting space for business-to-consumer (B2C) relations. From this, it follows that most of the virtual contracts concluded with a "point and click" procedure are "mass business contracts", with the business being subjected to mandatory information duties to be fulfilled in a certain form according to wether or not the counterpart is a consumer. The same is generally not true for smart contracting. In fact, the ideological foundation of and the technological solution provided by public blockchains such as Bitcoin, Ethereum, Waves and the countless projects that are currently being built on top of them offering smart contracting for the widest range of contractual relations, is based on the creation of a distributed, shared network with no single centre of control, but rather, where each participant contributes to the functioning of the whole system interacting directly with other "peers", without the need of third intermediary parties. As a consequence, most of the contractual relations enabled by the above-mentioned public blockchains should primarily be conceived as consumer-to-consumer relations, so that their validity and the validity of some of their contractual clauses is subjected to less restrictive formal requirements than those in force in B2C relations. Of course, businesses operating in several industries - mainly finance, banking, insurance and supply chain management - are getting increasingly interested in the huge benefits they could reap of the blockchain in terms of business performance, and their simplified and quick access to blockchain-based services is being enabled by projects like Azure Blockchain Workbench[87] and Corda[88]. For this reason, it is highly likely that

[87] On May 2018, Microsoft released a public preview of Azure Blockchain Workbench, its ready-to-use infrastructure made instantly available to businesses looking for a quick implementation of blockchain solutions. See more here: https://azure.microsoft.com/en-us/solutions/blockchain/

[88] A consortium of hundreds of world-class financial institutions the likes of Barclays, Bank of America, BNP Paribas is currently involved in the activity of R3, an enterprise software firm working to develop Corda, a distributed ledger technology inspired by the model of public blockchains but specifically designed to meet the needs of financial services industry. See more here: https://www.r3.com/

the blockchain infrastructure will soon turn into businesses' preferred means of interaction with their customer base, which raises concerns as to whether and how the same level of consumer protection currently prescribed by national and European legislation will be guaranteed in B2C relations regulated by smart coding, particularly in terms of informative duties and privacy. As to the latter, solutions to privacy concerns on the blockchain - especially following the entering into force of the new European General Data Protection Regulation 2016/679 on May, 25th 2018 - will briefly be illustrated in Part 3.

2.b. Conclusion of smart contracts ex article 1326, Civil Code. The rule of offer and acceptance

Other features of virtual contracts span from the theoretically global exposure of online contractual offers, which aim to be directed to the broadest audience possible of potential offerees, with the consequence that the terms of the agreements are typically unilaterally predisposed by the offeror, thus sacrificing any pre-contractual negotiation between the counterparts; that the content of such terms is as general as possible, since it cannot be customised to meet the needs of each single contractual relation; that the offerees are only left with the alternative between entering the contract as it is or not entering it all, which makes most virtual contracts perfectly fit under the contract formation procedure disciplined by our article 1336, Civil Code, on "Public Offer"[89].

Ultimately, the conclusion of virtual contracts, meaning the contractual phase stricto sensu, happens inter absentes and remotely, through the "point and click" procedure or qualified and digital signatures when so required by prescribed legal formalities.

In the contractual relations arising on public blockchains, lack of pre-contractual negotiation, unilateral predisposition of contractual terms from the offeror, generality of contractual clauses and formation through "Public Offer" ex art. 1336, c.c. are not the rule.

Several projects are being developed with an aim to facilitate the creation of smart codes tailored around the specific needs of single contractual relations, an example of which can be found in LegalThings One[90]. This project developed on top of the public blockchain Waves[91] allows the creation of Live Contracts, digital agreements formalised in a way that can be understood and processed by both humans and machines.

---

[89] According to article 1336, Civil Code, a public offer containing the essential elements of the contract it is directed to conclude equals to a formal contractual offer: "L'offerta al pubblico, quando contiene gli estremi essenziali del contratto alla cui conclusione e' diretta, vale come proposta, salvo che risulti diversamente dalle circostanze o dagli usi.
La revoca dell'offerta, se e' fatta nella stessa forma dell'offerta o in forma equipollente, e' efficace anche in confronto di chi non ne ha avuto notizia."

[90] See the white paper of the project here: https://docs.google.com/document/d/1hQTYt5UdnZg5dGZ65C7wqor4Yj75DcZy65SfQOE4Ab8/edit#heading=h.k4gnv5l15uvi. For more information on LegalThings One: platform for Live Contracts see: https://livecontracts.io/

[91] For more information on Waves blockchain see: https://wavesplatform.com/

Although Live Contracts are based on a set of static, predefined digital data corresponding to certain contractual clauses and machine instructions, new set of data can be added by the parties, or "actors", interacting with the contract through their public keys, thus leaving up some space to pre-contractual negotiation. The first actor initiating the agreement can add new parties by providing their public key and each party can contribute to the definition of the agreement by digitally signing each condition added to it. The digital agreement is deemed to be concluded once all parties have digitally signed the final version of the agreement, according to the finalising procedure which is itself defined by the contract's actors. A random SHA256 hash of the Live Contract is taken to uniquely identify the contract/code on the blockchain where it is stored.

In this case, the contract formation procedure is inter absentes and remote - two essential attributes of blockchain contracting as they are of online contracting - and follows the traditional rule of offer and acceptance set forth by articles 1326 ss., c.c.,[92] with the "meeting of the mind" being reached once the offer made by the first actor is accepted by the others in the form of a digital signature.

With the possibility for "hybrid" Live Contracts, or natural language, paper copy versions of the digital agreement carrying a handwritten signature of the parties, LegalThings One is among the most ambitious projects providing for a real-life application of the "Ricardian contract" concept elaborated in the 1990s by Ian Grigg[93]. According to such contracting model, a bridge can be created between the world of law and coding, with natural language contracts manifesting the parties' will to contract and specifying the terms and conditions of the agreement being uniquely identified through a hash function and digitally signed. At the same time, the hash of the legally binding electronic contract is linked to specific pieces of smart codes administering the data-driven performance of the contract.

In such an instance, the offer is accepted and the contract is deemed to be concluded once the offeree digitally signs the transaction referring to the hash of the contract, which will trigger execution from the smart code. Once more, the remote and inter absentes contract formation procedure can be referenced to the traditional rule of offer and acceptance of art. 1326, c.c.

Although a distinction must be drawn between smart coding and Ricardian contracts - with the former being a pure digital agreement that has already been agreed upon and can be executed automatically, while the

---

[92] According to the general rule of offer and acceptance posed by article 1326, c.c., a contract is deemed to be concluded at the time in which the offeror acknowledges the offeree's acceptance - which article 1335, c.c. presumes as soon as the letter of acceptance reaches the offeror's address, unless evidence of faultless impossibility of such an acknowledgement is provided - as long as the acceptance is timely and of the same content and form as that contained in or required by the offer, or it would amount to a new contractual proposal from the offeree to the offeror.

[93] See: Ian Grigg, *The Ricardian Contract*, First IEEE International Workshop on Electronic Contracting, 2004, pages 25 to 31

latter introduces an additional phase before the contract is automatically executed, which is the recording of "wet" elements such as the parties' will to contract and the terms and conditions of the agreement - more cross-fertilisation between these two contracting tools is desirable, resulting in the development of pre-defined standard contract templates understandable by humans whose execution is entirely driven by smart codes, thus offering the opportunity to prevent or solve some of the legal issues that may arise as a consequence of the reaching of a mutual assent or the definition of contractual clauses exclusively in a piece of code.

Conclusively, when the parties' will to transact through a smart code expressly results from a natural language - written or electronic - contract or from them taking part in a predefined digital procedure available online to conclude customised smart codes - regardless of the quality of business or consumer of such parties - the automatic execution of the contractual clauses by the smart code should not be effectively challengeable by any of the contracting parties on the basis of lack of mutual assent ex art. 1325, n.1, and a contract may be deemed concluded on the basis of the offer and acceptance rule ex art. 1326, c.c.

2.c. Conclusion of smart contracts ex article 1327, Civil Code. Execution of contractual terms before acceptance, or legally consequential conduct (comportamento concludente)

Nevertheless, there are also instances of smart codes executing unilaterally predisposed offers directed to unspecified, incertam persona offerees and lacking pre-contractual negotiation following the provision of art. 1336, c.c. "Public Offer".

The clearest example of this kind of smart contracting is OpenBazaar[94], a Bitcoin-based open source software developing a completely decentralised marketplace, which allows users to directly connect to the rest of the peer-to-peer network once they download the software, and start transacting as buyers and sellers. Its interface recalls the one Internet users are used to from surfing on any well-known centralised online markets such as Ebay or Amazon: sellers display pictures of their items and specify a price in a fiat currency (USD or EUR) - although payments happen exclusively in your pre-selected cryptocurrency -, the condition of the item and the terms of the shipping.

In such a scenario, rather than the rule of offer and acceptance described above, the procedure of "execution of contractual terms before acceptance" codified by article 1327, c.c. seems to provide for the best-fitting modality of conclusion of such a smart contract.

In derogation of the rule of offer and acceptance, article 1327 c.c. sets forth a simplified procedure for the conclusion of contracts, traditionally referred to by the Italian contract law doctrine and jurisprudence as "comportamento concludente", or "rebus ipsis ac factis", corresponding to cases of "legally consequential

[94] For more information on OpenBazaar see: https://www.openbazaar.org/

conduct", according to which a contract is deemed to be concluded at the time and place in which the execution of contractual terms contained in the offer is initiated by the offeree, without the need of a prior formal letter of acceptance. An information duty lies with the offeree to communicate the initiated execution to the offeror, with the aim of making him aware that a contract has been concluded and under penalty of compensation for possible damages suffered by the unaware offeror who has started separate negotiations or entered into other legally binding agreements.

Interestingly enough, the ratio legis of art. 1327, c.c. - as retraced by distinguished doctrine[95] - is perfectly reflected in the reasons for adoption and the potential benefits of smart contracts commonly put forward by their supporters, namely the need for readiness in a growing number of contractual relations - especially financial ones like buying orders, whose dependence on titles' ever-changing prices compels immediate action for their valid conclusion -; the reduction of transaction time and costs resulting from the elimination of unnecessary procedural burdens, in this case being a formal acceptance from the offeree; last but not least, conclusive actions may be aimed at neutralising the risk of revocation of contractual offers - which article 1328, c.c. considers ineffective once the contract has been concluded -, which recalls the feature of non-retractability characterising smart contracts.

Moreover, it is precisely a smart contract that an author[96] unawarely uses to describe a typical case of conclusive action ex art. 1327, c.c., when he states that the purchase agreement of goods from a vending machine - as well as any other purchase agreements concluded through automated systems, like refuelling at gas stations - is concluded once coins are inserted in the machine, without the need of the offeree's formal acceptance of the offer, unless one wants to embrace the general rule of offer and acceptance ex art. 1326, c.c., with the (inconvenient) consequence that this and contracts alike would only be deemed concluded once the offeror acknowledges the acceptance.

According to article 1327, c.c. the conclusion of contracts through execution before acceptance is valid only if at least one of the three requirements provided for the application of the simplified procedure is fulfilled. In particular, conclusive actions must have either been expressly required by the offeror, or demanded by the nature of the bargain or on the basis of current practices, including individual ones established within single contractual relations.

Smart contracts perfectly fit under this norm once the modality of their offer is considered: in fact, the circumstance that the conclusion (and automatic execution) of a smart contract is made promptly available on the offeror's website by inserting the offeree's public key - as it is the case on OpenBazaar and for most

95 E. Gabrielli, *Commentario del Codice Civile,* Dei Contratti in Generale, a cura di E. Navaretta e A. Orestano, artt. 1321-1349, UTET Giuridica, 2011

96 P. Gallo, Art. 1327 - Esecuzione prima della risposta dell'accettante, in Commentario al Codice Civile, note 1, pp. 308 ss.

smart contracts - may be considered equivalent to the offeror's express request of execution of the contract before acceptance.

Besides, with an estimated mainstream adoption of smart contracts since early 2020[97] by those industries which could hugely benefit from the time and costs savings resulting from their use, namely banking, finance and insurance, it shouldn't be an overstatement that the conclusion of certain agreements such as mortgages and insurance policies through "execution before acceptance" in the form of smart contracts will be demanded by the nature of the bargain itself.

Once the conditions under which the conclusion of a contract ex art. 1327, c.c. have been illustrated, the notion of "conclusive action" amounting to acceptance requires clarification. Doctrine and jurisprudence agree in demanding that the conclusive action be such to unambiguously express the offeree's acceptance of the offer, with the consequence that the offeree's omission to do something cannot amount to acceptance of an offer. Besides, conclusive actions expressing an unequivocal acceptance of the offer are required to be perfectly equivalent to the content of the offer, with the consequence that the case law of our Civil Supreme Court has deemed an execution slightly differing from that required in the offer to amount to a new offer made by the offeree to the previous offeror[98], and no contract to be concluded. On the other hand, part of our doctrine is more flexible in allowing the conclusion of contracts through initiation of execution even when the latter slightly departs from the request of the offeror.

The requirements of unambiguity of the conclusive action and its equivalence with the offer are perfectly met when a smart contract is concluded: the fact that the offeree is bound only once the smart contract has been signed off guarantees his unequivocal acceptance of the offer, and the automatic execution of contract clauses by the smart code guarantees their sheer compliance with the offer. In fact, in most cases the offeree won't be able to unilaterally integrate or edit the smart code, unless this faculty is expressly provided for by the code itself, in which case previous acceptance of the integration or editing by the offeror will be required which would amount to a new offer.

Another controversial question revolving around the notion of "conclusive action" is that of wether or not it shall be considered as a declaration of will from the offeree, which is not a mere classification issue without consequence. In fact, only once conclusive actions are recognised as having the same legal value as declarations of will, will the offeree be granted the traditional contractual remedies provided for in cases of legal incapacity and vices of consent. Our doctrine is still divided, with some part of it classifying conclusive actions among socially typical behaviours (comportamenti socialmente tipici), whose contractual relevance

---

[97] Capgemini Consulting Interview, June-July 2016, in *Smart Contracts in Financial Sector: Getting from Hype to Reality,* 2016: https://www.capgemini.com/consulting-de/wp-content/uploads/sites/32/2017/08/smart_contracts_paper_long_0.pdf

[98] See Italian Civil Supreme Court, n. 1508/1948, n. 3891/1969

is measured exclusively against the objective correspondence of the offeree's behaviour with that required by the offeror to conclude a contract[99], beyond any enquiry on the offeree's subjective will. A clear example of conclusive acts amounting to socially typical behaviours would be contracts concluded through automated systems: the mere fact of inserting coins in the machine or the fuel dispenser hose in the car concludes the agreement, with the consequence that the offeree won't be able to contest the contract in case of vices of consent or incapacity.

To soften the extreme consequences of such a classification, thus increasing the level of legal protection granted to offerees initiating execution through conclusive actions, the majority of our doctrine currently recognises them as having the same legal value as declarations of will, and allows for challenge of contracts concluded ex art. 1327, c.c. on the basis of lack of legal capacity and vices of consent.

As far as smart contracts are concerned, the recognition of their signing off - which corresponds to the initiation of execution - as having the same legal value as a declaration of will seems fitting. In fact, given the novelty of the tool, the theoretical irreversibility of its effects and the high sums that may be involved, it is of paramount importance that the highest level of legal protection possible is granted to the parties entering into them.

Last but not least, it should also be noted that extending the application of art. 1327, c.c. to the conclusion of smart contracts would reduce, if not completely eliminate, any ambiguity regarding the time and place of contract formation, since they would be readily knowable through geolocation of IPs, and that the information duty lying on the offeree to communicate the initiation of execution to the offeror could be promptly fulfilled by the sending of an automatic email to the offeror's address as soon as the smart contract has been signed and executed.

Conclusively, as far as the essential requirement of a mutual assent to contracting through smart coding is concerned, this can be fulfilled either through (1) the traditional rule of offer and acceptance ex article 1326, Civil Code, (1.a) with the parties concluding a natural language - electronic or written - version of the contract remitting the execution of the agreement to pieces of code or (1.b) with the parties developing their whole contractual relation, including pre-contractual negotiation, on a smart contract platform such as LegalThings One, with the contract deemed to be concluded once all parties have digitally signed the final version of the smart agreement. Alternatively, the meeting of the mind may occur on the basis of (2) the simplified procedure of article 1327, Civil Code, with the digital signature of the code by the offeree amounting to a case of "execution before acceptance". In such an instance, however, it is vital that at least the essential elements of the offer are defined in a language understandable by the offeree for the execution

[99] Sacco, De Nova, *Il contratto*, 3 ed., Torino, 2004

to amount to lawful acceptance, as it is required by the provision on "Public Offer" of article 1336, Civil Code and exemplified by decentralised platforms such as OpenBazaar.

3. Can smart contracts fulfil the formal requirement prescribed for specific contracts by article 1325, (4) Civil Code?

After illustrating how the essential requirement of a "meeting of the mind" ex article 1325, n. 1 can be reached between parties to a smart contract, this paragraph will enquire whether and how smart contracts can satisfy the legally prescribed formalities for the validity of some contracts (ad substantiam) and for evidence of the contracts' existence and of the parties' consent in legal proceedings (ad probatiotem). It will do so by offering an extensive interpretation of the current European and national legislation regarding electronic documents and electronic signatures, with an aim to show that blockchain-based smart contracts fit under the above-mentioned legislation, thus respecting the legal form required of some contracts.

The recourse to an extensive interpretation of the existing legislation on related subject matters is made necessary by the absence of any express provisions on such a topic in our legal system at the time of writing. In fact, in Italy the discussion regarding the blockchain technology and its potential applications is falling behind the progress already made by other States, like the USA - with Arizona[100] and Vermont[101] having passed groundbreaking laws which go so far as to openly recognise the legally binding force of smart

---

[100] On March, 29, 2017, House Bill 2417 was signed into law by Arizona Governor, which clarifies that smart contract terms secured through blockchain technology will be considered to be in electronic form and to be an electronic signature under the Arizona Electronic Transactions Act ("AETA"), which previously provided only for records or signatures in electronic form and stipulates that they cannot be denied legal effect and enforceability based on the fact they are in electronic form. Additionally, HB 2417 provides that contracts relating to the sale of goods and leases may not be denied legal effect, validity or enforceability solely because they contain a "smart contract term". See the amendments to AETA adopted by HB 2417 here: https://legiscan.com/AZ/text/HB2417/id/1588180

[101] On July, 1 2016, Section I.1 (blockchain technology) of House Bill 868 took effect in Vermont, with the aim of allowing for broader business and legal application of blockchain technology to promote economic development. After providing a definition of the blockchain technology, the Bill sets forth the conditions for the authentication and admissibility of digital records electronically registered in a blockchain and the presumptions applying to such records, among which stands out the presumed authenticity of facts or records verified through valid application of blockchain technology to determine "contractual parties, provisions, execution, effective dates, status" (Sec. I.1, lett. c, 1) as well as "the ownership, assignment, negotiation, and transfer of money, property, contracts instruments, and other legal rights and duties" (Sec. I.1, lett. c, 2). See House Bill 868 here: https://legislature.vermont.gov/assets/Documents/2016/Docs/ACTS/ACT157/ACT157%20As%20Enacted.pdf

contracts - and France[102]. Italy is not even keeping up with the initiatives fostered at the European level, since it was not one of the signatories of the 2018 Declaration on the Establishment of a European Blockchain Partnership[103] entered into by twenty-two Member States. In this regard, it would be desirable if Italy joined the European and international cooperation on the "potential of blockchain-based services for the benefit of citizens, society and economy"[104] by supporting the discourse both at the academic and political level.

3.a. Relevant European and domestic legislation on electronic documents and e-signatures

Following the rise of contractual relations on the Internet (e-commerce) in the past decade, the European Union intervened to harmonise the often-contradictory patchwork of laws governing electronic commerce transactions enacted by its Member States. The resulting European pieces of legislation pertaining to this analysis are the Directive on electronic commerce 2000/31/EC[105] - implemented in our legal system through d. lgs. n. 70/2003[106] - and the so-called eIDAS Regulation

---

[102] With Ordonnance n° 2016-520 of April, 28th, 2016, the legal framework applicable to interest-bearing notes ("*bons de caisse"*, literally "deposit bonds") was modified with the introduction of the ability to issue, subscribe and assign an interest-bearing note using a distributed ledger. New article L223-12 of the French Monetary and Financial Code defines a distributed ledger as a "shared mechanism of electronic recording which allows the authentication of these transactions, within security conditions" which will be defined in a future decree, and new article L223-13 of the same Code acknowledges the validity of interest-bearing notes' assignment using distributed ledger technology, which is deemed to replace the mandatory written agreement, the debtor being notified of the assignment directly through the relevant distributed ledger. For an overview on the recent amendment to the French Monetary and Financial Code see: https://www.davispolk.com/files/2017-12-18_france_allow_use_blockchain_technology_unlisted_securities.pdf

[103] Following the invitation of the European Council to the European Commission to put forward initiatives for strengthening the European approach to blockchain, on April, 10, 2018, twenty-two Member States agreed to cooperate in the establishment of a European Blockchain Partnership "with a view to developing a blockchain infrastructure that can enhance value-based, trusted, user-centric digital services across borders within the Digital Single Market" and recognised "the potential of blockchain to transform digital services in Europe". See the scanned original document with signatures following this link: https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership

[104] See Declaration on European Partnership on Blockchain

[105] Dir. 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32000L0031

[106] D. Lgs. April, 9, 2003 n. 70, Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno: http://www.interlex.it/testi/dlg0370.htm

910/2014[107], which repealed the Electronic Signature Directive 1999/93/EC - whose differing interpretation by the Member States had complicated the common validity and recognition of e-signatures throughout the EU, thus hindering the consolidation of a Digital Single Market - and entered into force on July, 1, 2016 thus establishing a directly applicable common legal framework in the EU. Italy harmonised its previous legislation to the new eIDAS Regulation by amending the Code of Digital Administration d. lgs. n. 82/2005 through d. lgs. 179/2016[108].

A pivotal provision of Dir. 2000/31/EC is article 9, stating that: "All Member States shall ensure that their legal system allows contracts to be concluded by electronic means. Member States shall in particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means".

Our legal system was already compliant with such a provision, with article 15, (2), law 59/1997[109] recognising electronic or telematic deeds, data, documents and contracts from both the Public Administration and private parties as valid and fully legally effective, including their electronic archiving and transmission[110]. Italy implemented Dir. 2000/31/EC through d. lgs. 70/2003, which laid down the legal requirements applicable to e-contracts, such as the general (article 7) and supplementary mandatory information (article 12) that providers are required to provide to their service's recipients and consumers, and prescribed the application of the general rules on contract conclusion (articles 1321-1469*sexies,* Italian Civil Code) to e-contracts (article 13,(1).

A detailed illustration of the legal requirements for the different types of e-commerce (B2B, B2C, C2C, etc.) is beyond the scope of this paragraph. Here suffices it to refer to the main provisions ruling on the form, validity and legal effectiveness of e-documents and e-signatures.

---

[107] Reg. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

[108] D.lgs. March, 7, 2005 n. 82, Codice dell'amministrazione digitale, aggiornato al decreto legislativo 13 Dicembre 2017, n. 217: http://www.bosettiegatti.eu/info/norme/statali/2005_0082.htm

[109] Law March, 25, 1997 n. 59: Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione normativa: http://www.camera.it/parlam/leggi/deleghe/00443dla.htm

[110] Article 15, (2), law n. 59/1997: "Gli atti, dati e documenti informatici formati dalla PA e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici sono validi e rilevanti a tutti gli effetti di legge"

Articles 1(b), T.U. 445/2000 and 1(p) d. lgs. 82/2005 agree in defining e-documents in our legal system as the "representation of deeds, facts and other legally relevant data in electronic form". Their legal validity and effects have recently been reiterated at the European level by the fundamental principle of equivalence between paper and e-documents of article 46 of the eIDAS Reg, according to which: "An electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form". What needs to be determined, however, is under what conditions e-documents may be deemed compliant with the formal requirements provided for certain types of legal acts. Since such requirements are fulfilled by the signing of the acts by their author, the legal relevance of e-documents is dependant on the degree of reliability of their signature[111].

At the European level, article 3 of the eIDAS Regulation currently recognises three different types of e-signatures: "simple" e-signature, corresponding to electronic data "attached to or logically associated with other data in electronic form and which is used by the signatory to sign" - examples are online credentials, PINs, or even name and surname of the sender at the end of an email; advanced e-signature, a simple e-signature fulfilling the additional requirements of art. 26, eIDAS Reg.[112]; qualified e-signature, or an advanced e-signature (a) created by a qualified e-signature creation device and (b) based on a qualified certificate for e-signatures. As to their level of reliability and the resulting legal effects of the e-documents they are attached to, article 25, eIDAS Reg. makes a clear distinction: as far as simple e-signature is concerned, it is provided that its legal effects and admissibility as evidence in legal proceedings shall not be denied "solely on the grounds that it is in electronic form or that it does not meet the requirements for qualified e-signatures", thus leaving it up to domestic legislations to determine its legal effects. On the other hand, advanced and qualified e-signatures are held to be equivalent of handwritten signatures, so that any laws requiring written form for an act to deploy its legal effects are fulfilled by both types of e-signatures.

Italy has updated its legislation on e-documents and e-signatures by amending article 20, Digital Administration Code, which currently provides that: e-documents signed with advanced, qualified or

---

[111] V. Roppo, Il contratto, Giuffré Editore, 2011, pp. 227-230

[112] Advanced electronic signatures shall be: (a) uniquely linked to the signatory; (b) capable of identifying the signatory; (c) created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; (d) linked to the data signed therein in such a way that any subsequent change in the data is detectable

digital[113] e-signatures comply with the written formal requirement and have the same probative effect as a private writing ex article 2702, Italian Civil Code. As to not signed e-documents and those signed with simple e-signatures, their validity and probative effect shall be freely assessed by the judge on a case by case basis, considering their objective characteristics of quality, security and integrity. Moreover, article 21, (2bis), DAC prescribes - under penalty of voidness - the use of qualified, digital or advanced e-signatures for electronic documents to meet the form requirement of article 1350, n. 1-13, Civil Code, while article 21, (2ter), DAC prescribes - once more under the penalty of voidness - the use of qualified or digital e-signatures from the public notary on electronic public deeds.

3.b. How do smart contracts fit under these pieces of legislation?

The key to extensively interpret the current legislation on digitally signed e-documents in favour of blockchain-based smart contracts lies in the cryptographic key with which they are signed and acknowledged. In fact, the asymmetric key encryption of digital signatures - which assures the origin and integrity of the e-document they are attached to and gives it validity and full legal effectiveness in our legal system - is exactly the same mechanism used by parties to express their consent to blockchain-based smart contracts, as described in Part 1[114]. For this reason, the fact that parties to a smart contract have signed it through their cryptographic keys should assure courts that the legally prescribed formal requirements have been fulfilled by the same technology used to validly sign electronic contracts according to our current legislation.

One objection to this position may arise: since public blockchains' users operate mostly under anonymity or pseudonymity, the asymmetric encryption used to sign smart contracts would not fall under the notion of digital signature on the grounds that the identifiability of the signor is not guaranteed. The most appropriate response to such an objection seems to be that (1) there are several public blockchain-based start ups currently trying to tackle the identity issue on the blockchain (some of which will be mentioned in Part 3) and that (2) if the signing off on smart contracts is not deemed to be equivalent to any of the typical signatures required by our legislation to fulfil formal requirements, then the the validity and legal effectiveness of the smart contract will be freely assessed by the judge

[113] Digital signatures were introduced in our legal system by D. P. R. n. 445/2000, Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (http://www.camera.it/parlam/leggi/deleghe/00443dla.htm) and represent an Italian peculiarity in the field of e-signatures. They are highly secure e-signatures based on asymmetric or double-key cryptography, which allow the signatory using the private key and the recipient using the public key, to assure the origin and the integrity of an electronic document or a set of electronic documents.

[114] See Chapter 1, from p. 5

on the basis of the objective attributes of "security, quality and integrity" guaranteed by the tool used to sign the smart contract. In such an instance, in their case by case valuation judges shouldn't ignore that enhanced security, quality and integrity are precisely the distinguishing features of the blockchain technology as a contracting tool. Moreover, as to the assessment on whether and through what procedure a mutual assent between the parties to a smart contract has validly been reached, reference is made to the previous paragraph.

4. Smart coding as a suitable tool to express the "economic operation" of contracts

So far, this dissertation has argued that the blockchain and smart contracts could be seen as an alternative, decentralised solution to the same problem of trust among distrustful counter-parties that originally spawned the centralised solution of traditional contract law. Subsequently, smart contracts have been analysed from a traditional contract law perspective in order to assess if - and with what precautions - they can be deemed to meet the foundational requirement of a "meeting of the mind" ex art. 1325, (1) Civil Code and the formal requirement provided for specific contracts by art. 1325, (4) Civil Code.

This paragraph will briefly illustrate the doctrinal and case law evolution in defining the notion of contractual "cause" ex art. 1325, (2), Civil Code, as well as introduce the new contractual category of "economic operation" which spawned from such a notion and rose to a new interpretative device of contractual clauses. It will do so with the aim to suggest that smart contracts could be seen as an appropriate tool to clearly outline the "economic operation" that the parties wish to realise through their agreements.

The elaboration of the concept of "economic operation" as an autonomous contractual category[115] spawned from the doctrinal and case law evolution regarding the definition of contractual "cause". Although article 1325, Civil Code, n. 2 includes a "legitimate cause" among the essential elements of contracts, no univocal definition of it has been given by the Legislator, with the consequence that our commentators and judges took up the task of specifying such a notion. Traditionally, the "cause" was equalled to the objective "economic-social function" that each contract aimed at realising, regardless of the subjective, individual intentions and programmes of the contractual parties. From this characterisation of the notion, it followed that each contract could be made fit under a specific "type", previously elaborated and regulated by national laws[116]. Successively, however, a different perspective on the notion of "cause" was offered by those authors[117] emphasising the relevance of the parties' "practical" intentions in the definition of their economic

---

[115] Roppo, see note 111

[116] The most authoritative elaboration of the notion of cause as the economic-social function of the contract was given by E. Betti, *Teoria generale del negozio giuridico,* Camerino Rist. 1994, 170 – 207, and *Causa del negozio giuridico,* in *Noviss. Dig. It.* III, Torino 1957, 32 ss

[117] Giovanni B. Ferri, *La cause nella teoria del contratto*, in Ferri e Angelici, *Studi sull'autonomia dei privati*, Torino, 1997, 99

interests[118], which resulted in the specification of the contract's "cause" as the "economic-individual function" it is aimed at fulfilling and in the breaking of that previously necessary and unbreakable link of any single contract to a pre-regulated type. The "practical" function that contracts aim at realising according to such a framing of the notion of "cause" is better enunciated and described by referring to the single "economic operation" pursued by the contract, or the bargain, the economic result that the counterparts mean to achieve through the transaction[119]. On this basis, a distinction has been drawn between, on one side, the notion of "contract" intended as "juridical formalisation" of, on the other side, "the situations, relations, interests that build the real substance of each contract and make up its economic operation"[120]. The conceiving of an "economic operation" as an autonomous contractual category had an impact on the interpretation of contracts. The subjective and ambiguous notion of the parties' "will" as the foundation element of contracts and main method to define the meaning of contentious contractual clauses has given way to the more objective target of the economic operation they aim at realising. Consequently, the "economy" of contracts has acquired an undisputed central position, while the "will of the parties" as the foundational element of contracts has gone through a likewise indisputable decadence[121].

Such a notion of "economic operation" has been defined as "the objective setting within which the terms set by the parties and their behaviours aiming at reaching the desired economic outcome take place"[122] and the reason for its increased importance in the doctrinal formulation of contracts lies in that line of reasoning based on the assumptions that: i) contracts fulfil a primarily economic function; ii) contracts, inasmuch as they aim at realising an economic program, have a patrimonial cause which is objectively definable (and as such, independent from the parties' "subjective will")[123]. From this, it follows that in assessing the content and scope of legal transactions, priority should be given to a "functionalist" approach taking into account

---

[118] E. Gabrielli, *"Operazione economica" e teoria del contratto, Studi,* Giuffré Editore, 2013, p. 68: "Il contratto, ogni contratto, è in definitiva quello che risulta dalla sua causa in concreto, ed il tipo esprime soltanto un modello di organizzazione degli interessi."

[119] Ibid: "La rilevanza che in concreto, in ogni singola fattispecie, la funzione dell'atto assume viene resa più evidente attraverso il concetto di operazione economica, poiché è sul piano del fatto, dell'affare, considerato e valutato in tutte le sue componenti tipologiche, morfologiche e funzionali che occorre volgere l'indagine per comprendere in pieno il valore ed il significato dell'affare dei privati e la disciplina che lo governa".

[120] Roppo, *Il contratto*, in *Trattato Iudica e Zatti*, Milano, 2001, p. 73: "Le situazioni, i rapporti, gli interessi che costituiscono la sostanza reale di ogni contratto si possono riassumere nell'idea di operazione economica (…). Con il termine "contratto" non ci si riferisce tanto alle operazioni economiche concretamente realizzate nell'effettiva esperienza dei traffici, ma piuttosto a quella che potremmo chiamare la loro formalizzazione giuridica".

[121] See M. Grondona, *Diritto dispositivo contrattuale. Funzioni, usi, problemi*, Giappichelli Editore, 2011 p. 173

[122] E. Gabrielli, *Il contratto e l'operazione economica*, in Riv. dir. civ. 2003, I, p.93

[123] See M. Grondona, note 121, p. 172: "ii) se il contratto, in quanto operazione economica, ha (come in effetti ha) un nucleo di significato economicamente rilevante sotto il profilo oggettivo (dunque autonomo rispetto al "voluto soggettivo" delle parti) (…)"

their patrimonial cause and directed towards the "practical realisation of their cause"[124], rather than to the mingling of parties' intensions expressed through the contract terms, referred to as their "subjective will", which will add up to national contract norms thus resulting in what is, more often than not, a hardly harmonic regulatory setting[125]. Such a position is exemplified by a 2016 decision from the Italian Civil Supreme Court[126] according to which in interpreting binding agreements, the literary meaning of the clauses should be evaluated from a primarily functionalist standpoint which priorities the "practical aim" the contract is directed towards and is considerate of the patrimonial interests the parties are looking to protect through it.

The climax of such "economically-oriented interpretation of contracts"[127] is reached by those scholars attributing paramount importance to the "practical economic operation estimated in its formal unity"[128] and asserting that "the economic operation represents the parties' autonomy at its deepest, beyond the forms employed by the parties to define it and the exterior representation of the layout they have adopted"[129].

The above-mentioned evolution of contract theory from a primarily subjective to a more objective evaluation of contracts cannot be ignored when one wonders whether smart contracts should be recognised as appropriate contracting tools.

As a matter of fact, if such a functionalist approach is endorsed which favours the interpretation of contracts on the basis of the individual economic program they aim at performing, the convenience of using a tool whose main feature lies in its ability to turn intentions into objective instructions directed towards the production of a clear economic outcome should not be underestimated.

As already pointed out in Part 1, smart contracts should simply be intended as "smart codes" recorded on the blockchain that automatically execute themselves when certain conditions previously set in the code itself arise. The notion of "contract" comes into play when such smart codes have an economically valuable "object" (money or other assets such as property or IP rights), or are aimed at the realisation of a specific economic program, which would justify the creation of a traditional legally binding agreement to ensure that

---

[124] Ibid

[125] E. Russo, *Il termine del negozio giuridico*, Milano, Giuffre, p. 90, nota 158

[126] Cass. n. 23701/2016. "In tema di interpretazione del contratto, l'elemento letterale, sebbene centrale nella ricerca della reale volontà delle parti, deve essere riguardato alla stregua di ulteriori criteri ermeneutici e, segnatamente, di quello funzionale, che attribuisce rilievo alla "ragione pratica" del contratto, in conformità agli interessi che le parti hanno inteso tutelare mediante la stipulazione negoziale".

[127] See M. Grondona, note 121, p. 172

[128] E. Gabrielli, *L'operazione economica nella teoria del contratto*, in Riv. trim. dir. proc. civ., 2009, pp. 905 ss.: "Al di là del tipo opera (…) la disciplina dell'auto-regolamento dei privati interessi: cioè la concreta operazione economica nella sua unità formale. (…) L'operazione economica esprime, al di là delle formule impiegate dalle parti per definirla e della raffigurazione esteriore dello schema adottato, il significato più profondo del potere di autonomia riconosciuto ai privati".

[129] Ibid

the parties be able to enforce the terms[130]. Such a characterisation highlights the fundamental role played by coding in the definition (and execution) of smart contractual terms, which is opposed to the use of natural language or legalese in the definition of traditional contract terms. While the latter is directed towards human communication and pays the price of its generality and open-meanings, often resulting in a need for interpretation which is, by definition, subjective and approximative, coding as a programming language is used to instruct machines and is necessarily characterised by simplicity, univocality and determinism. As a consequence, codifying contractual terms through code should be regarded as a better-suited tool to express the economic programmes that the parties aim at realising, since it would force them to clearly and exclusively represent the objective economic operation they want to enact by translating their common will into specific instructions.

Smart code seems to be the most accurate tool to translate subjective intents into clear economic operations, and if the latter represent, as mentioned above, "parties' autonomy at its deepest, beyond the forms employed by the parties to define it and the exterior representation of the layout they have adopted", smart contracts - which meet the other formal requirements discussed in the previous paragraphs - should be deemed to have legally binding force upon their parties.

With this being said, some scholars go so far as to claim that the existing rules on the interpretation of the contract do not apply to smart contracts ("Interpretation according to the common intention of the parties and not only on the basis of the words' literal meaning")[131], since the code itself is meant to be the ultimate arbiter of "the deal" it represents without being subjected to interpretation by outside entities or jurisdictions[132].

Nevertheless, the relevance of subjective intent in and the need for a natural language version of smart codes that can be understood by the parties and judges should not be excluded *a priori,* which strengthens the argument that the successful use of smart coding as a contracting tool will ultimately be measured against the level and quality of the cooperation established between legal practitioners and programmers. The former will have to bridge the huge gap of abstraction between legal and programming language, by taking part in the drafting of smart codes to ensure that they represent the exact implementation of a certain contractual type[133], advising their clients on which is the best-suited smart contract on the basis of their specific needs and provide its natural language version. The natural language version and the smart code should create an *unicum*, so that if the latter is subjected to flaws or bugs resulting in its non or incomplete performance, the former will act as a reference for judges or arbitrators to retrace the parties' common will.

---

[130] See Part 1, p. 21

[131] See art. 1362, 1, Civil Code. Intention of the parties

[132] See Savelyev, note 21, p. 14

[133] G. O. Hernandez, *Magic circle firms double down on legal smart contracts, on Legal Week*, Apr. 2018: http://www.legalweek.com/2018/04/03/magic-circle-firms-double-down-on-legal-smart-contracts-378-79500/

Programmers, on the other hand, will be responsabile for providing the technical implementation of contractual types, which rises the question of determining the liability for damage caused by flaws or bugs in the code covered in Part 3.

With this being said, one could argue that smart contracting could be seen as the natural evolution of that line of thought prioritising the "function", or their objective economic content, over the more ambiguous notion of "subjective will" as the foundation element of a contract, and on the basis of such a doctrine, the question as to whether or not contracting parties could legitimately regulate their economic interests through them should be given a positive answer.

Even if one does not embrace the above-mentioned doctrinal approach in interpreting contracts and its conclusions as to the opportunity of recognising smart contracts as legally binding agreements between their parties, some authors have argued that the features of coding as a language are such that another path can be taken to get to the same point[134]. In fact, the computer languages on which smart contracts are drafted inherently have conditional nature in that they are based on statements like "if X then Y". Such an approach is completely fitting with contractual terms and conditions, as confirmed by the position of those scholars considering the enforcement of a contract "nothing more than the running of a circumstance through a conditional statement"[135]. In this regard, smart contracts could be classified as conditional contracts under the existing taxonomy of Italian contract law as per art. 1353 of our Civil Code.

Conclusively, a final remark is needed to object to the extremist position of those asserting that "Strictly speaking, smart contracts don't have a need in a legal system to exist: they may operate without any overarching legal framework"[136].

Although it is true that mathematics and cryptography are universal languages which could make smart contracts truly transitional and uniformly executable regardless of the differences in national laws, thus eliminating the need of conflict of laws provisions; that coding is a univocal language whose implementation in contracting would drastically reduce, if not eliminate, the need to recourse to interpretation rules, one should not make the mistake of considering traditional contract law exclusively as a hindrance to the full realisation of individual economic goals, which would better be fulfilled by other means. Arguably, contracts are a comprehensive economic and juridical entity within which the stability of the economic relation is guaranteed by national contract norms and the parties' lex contractus. Without such a guarantee from the legal system, the needs and goals of the economic relations would be frustrated. In contracts, legal regulation

---

134 See Savelyev, note 21, p.15, where he states that: "In this regard Smart contracts fall within the existing taxonomy of contract law" as far as Russian contract law is concerned

135 M. Raskin, see note 40

136 See Savelyev, note 21, p. 21

and economic operation make a *unicum* within which none of them can be conceived as individually without voiding the other of its meaning.[137]

In other words, the principles and notions elaborated by traditional contract law are essential even when the execution of agreements is delegated to machines. In order for a smart contract to transfer property, IP or any other rights, there must be a shared definition of what such a right is and what it entails, and that definition is provided by traditional contract law. Even the most committed smart contract supporters should recognise that contract law has always displayed an inherent ability to adapt to new situations without the need for major revisions of its underlying principles and that "technology - while not changing contract law - adds complexity to the traditional analysis"[138]. Although the blockchain and smart contracts are undoubtedly among the technological advancements adding the most complexity to traditional contract law, they won't determine its fading but rather, they will raise the question of how to make the traditional analysis applicable to them and it is on the law to give the most appropriate answer.

From this, it follows that what had previously been presented as a dichotomy between centralised and decentralised solutions to contracting can now be reframed as a mutually-enriching relation with strong potential benefits to the definition of contractual relations:

Solution to the problem of trust among distrustful counter-parties

	Centralised solution	Decentralised solution
Entity enforcing agreements	State	Blockchain
Tool for contracting	Traditional contract law	Smart contracts
	Integrated by	Integrated by
	Smart contracts ↓	Principles of traditional contract law ↓

Smart contracts and traditional contracting are not to be conceived as alternative and conflicting solutions, but rather as mutually-beneficial tools for the definition of contractual relations

[137] A. D'Angelo, *Contratto e operazione economica*, G. Giappichelli, 1992, pp. 59-60

[138] E. Milk, "Formation Online", 159, in M Fumston and G J Tolhurst, *Contract Formation: law and practice*, OUP, 2010

5. Considerations on the recent evolution of the Italian case law on buying orders

This paragraph illustrates the recent evolution in Italian case law and doctrine regarding the relationship between master agreements ("contratti relativi alla prestazione dei servizi di investimento" according to article 23, T.U.F., *see below)* concluded between investors/clients and their brokers and the single financial orders entered into on the basis of the former, which seems to be moving towards the recognition of financial orders as having independent contractual force rather than being mere execution acts of the initial master agreement.

The aim of this analysis is to try to extend the thesis of the contractual nature of financial orders to buying and selling smart orders concluded on a blockchain in order to argue in favour of their legally binding force.

For the purpose of this analysis, reference will be made to financial orders transmitted to and executed by institutional brokers such as banks, non-bank financial institutions (Sim, Sicav, Sicaf), hedge funds and other juridical and physical persons offering financial services according to the definitions provided by article 1, *d-quater* et seq., d. lg. n. 58/1998, also known as Finance Consolidated Act[139].

Through financial orders, investors manifest their will to buy or sell titles (stocks, government bonds, etc.) by communicating the order to their brokers who will be responsible for its execution on a trading venue (regulated market (RM), multilateral trading facility (MTF), organised trading facility (OTF) selected on the basis of the brokers' "execution strategy"[140], previously agreed upon by their clients and aimed at guaranteeing the best conditions for investors when executing their orders.

The validity of such orders is conditioned upon the existence of a preceding valid master agreement between the client and the broker in which the terms of the future brokering activity are set out by the parties. The necessary content of such a contract is outlined in article 37, (2), *a-i,* CONSOB Regulation 16190/2007[141], and article 23, T.U.F. requires that the contract be in writing *ad substantiam[142].* Furthermore, a paper or electronic copy of the agreement must be given to the investor for informative and evidentiary purposes.

Case law and doctrine agree in considering master agreements as "framework agreements whose cause is the prearranged regulation of an indefinite amount of contractual transactions - to which, however, no

---

[139] Testo Unico della Finanza (T.U.F.), d. lgs. February, 24th, 1998, n. 58. See the updated version here: http://www.consob.it/documents/46180/46181/dlgs58_1998.pdf/e15d5dd6-7914-4e9f-959f-2f3b88400f88

[140] For more information about the content of and agreement upon execution strategies, see articles 45-46, TUF

[141] CONSOB, Regolamento intermediari, n. 16190/2007. See the updated version here: http://www.consob.it/documents/46180/46181/reg_consob_2007_16190.pdf/bad28615-4a2c-40d0-b130-551000f26cdc

[142] With decision n. 898/2018 , our Civil Supreme Court ruled that the master agreement is valid and the written formal requirement met when the contract is signed only by the investor/client and a copy is provided to him, thus considering the lack of the broker's signature irrelevant as to the meeting of the formal requirement.

transaction might as well follow - and aiming at making a broker's business organisation available to his clients"[143]. However, a debate regarding the juridical nature of master agreements is still open, whose solution does not come without consequences as to their relation with single financial orders and the classification of the latter as contracts or not.

According to the prevailing thesis, master agreements fit under the agency contract type, with the consequence that the single financial orders concluded by the broker on his client's behalf amount to mere executive acts of the master agreement, which is the only one to be recognised as having contractual force[144]. Nevertheless, conflicting decisions have recently been adopted by first instance courts which seem to disprove the classification of master agreements as agency contracts, arguing that while agency contracts admit a certain degree of indefiniteness as to their content - so that the initial regulation of the principal-agent relation may be integrated by additional instructions from the former to the latter when so required by specific situations - master agreements are characterised by sheer indefiniteness, given that their content is completely defined on the basis of the investor's single manifestations of will expressed through financial orders[145]. This thesis has been embraced by recent doctrine who stressed out the fundamental discrepancy between agency and master agreements lying in the fact that the latter are "empty" agreements, whose content needs to be defined by future manifestations of will in the form of financial orders by investors[146]. An additional step away from the classification of master agreements in terms of agency agreements was taken by article 23(6), which demands "specific diligence" of brokers carrying out financial operations on

---

[143] See Milan Court, decision n. 7076/2012: "accordo normativo o programmatico la cui causa consiste nel regolare in via preventiva una indefinita serie di negozi - a cui tuttavia potrebbero anche non seguire operazioni di investimento - e con cui l'intermediario pone la sua organizzazione di impresa a disposizione del cliente".
Of the same idea is F. Durante, *Intermediari finanziari e tutela dei risparmiatori,* Giuffré, Milano, 2009, p. 42, who describes master agreements as: "intesa con la quale intermediario e cliente predispongono una dettagliato regolamento contrattuale che costituisce la cornice all'interno della quale si iscriverà la conclusione di futuri (e soltanto eventuali) atti giuridici".

[144] Italian Civil Supreme Court (SS.UU), n. 26724/2007: "Dal "contratto quadro", cui può darsi il nome di contratto d'intermediazione finanziaria e che per alcuni aspetti può essere accostato alla figura del mandato, derivano dunque obblighi e diritti reciproci dell'intermediario e del cliente. Le successive operazioni che l'intermediario compie per conto del cliente, benché possano a loro volta consistere in atti di natura negoziale, costituiscono pur sempre il momento attuativo del precedente contratto d'intermediazione."

[145] See Venice Court, decision n. 606/2007: "il mandato tollera un certo grado di indeterminatezza nel suo contenuto, nel senso che il regolamento iniziale può essere integrato a volta a volta che le esigenze lo richiedono a mezzo di istruzioni impartire dal mandante, tuttavia il contratto quadro presenta un livello assoluto di indeterminatezza poiché il suo contenuto sarà determinato integralmente di volta in volta da manifestazioni autonome di volontà del cliente"

[146] G. Bersani, *La responsabilità degli intermediari finanziari,* UTET Giuridica, p. 153

their client's behalf, as opposed to the provision of article 13 of law n. 1/1991[147] which previously required that brokers acted according to the same level of diligence demanded of agents towards their principals.
This juridical estrangement of master agreements from agency agreements resulted in the reconsideration of financial orders from mere execution acts of the foundational, preceding master agreement to autonomous contracts having legally binding force. As Ravenna Court of first instance put it: "single financial orders represent autonomous contracts whose object is the rendering of financial services"[148].
Seen in this new perspective, the relation between brokers and their clients/investors is articulated into two functionally connected although distinct contractual phases: the first one marked by the conclusion of the master agreement, and the rest of it being defined by the single financial orders (contracts) concluded by the broker on his client's behalf.
In fact, it has been argued that the executive function of finance orders within the broker-client relation does not necessarily imply the exclusion of their contractual nature, with the consequence that finance orders - and not only the master agreement - can be deemed to be subjected to contractual remedies like declaration of invalidity, termination in case of non-performance and all the consequences related to the breach of duties prescribed by sectoral legislation[149].
All in all, it is precisely through single finance orders that investors manifest their will to conclude investment operations by defining the title they intend to transact on, its amount and price, with the

[147] Disciplina dell'attività di intermediazione mobiliare e disposizioni sull'organizzazione dei mercati mobiliari, Law January, 2nd, 1991 n. 1: http://www.gazzettaufficiale.it/eli/id/1991/01/04/091G0003/sg . It is worth mentioning that decision n. 26724/2007, Civil Supreme Court, SS.UU. mentioned in note 8 was adopted under the effect of law n.1/1991 and before the entry into force of the new discipline provided by article 23(6), T.U.F.

[148] See Ravenna Court, decision n. 1885/2009: "i singoli ordini di negoziazione danno luogo alla formazione di contratti e questi contratti hanno per oggetto la prestazione di servizi di investimento"

[149] See Cuneo Court, decision n. 358/2012: "la finalità esecutiva dei singoli atti posti in essere nell'ambito del rapporto di intermediazione finanziaria non escludono la natura negoziale con conseguenza di agire per la dichiarazione di risoluzione per inadempimento dell'ordine"

consequence that finance orders have all the essential requirements of a contract, namely manifestation of will, cause, and object[150].

The relevance of such a digression with regard to smart contracts lies in the fact that it seems to open up a path to the opportunity of arguing in favour of the contractual nature of buying and selling smart orders concluded on a blockchain. Given the increasing interest shown by global financial institutions into the potential applications of private blockchain and distributed ledger technology to their industry[151] it is important to enquire as to wether or not buying or selling smart orders can be recognised as having contractual force, while keeping in mind that a positive answer to this question would result in a series of contractual remedies made available to investors transacting through blockchain-based financial institutions. On the basis of the described thesis of the autonomous contractual force of financial orders - according to which it is precisely through the single financial order that investors manifest their will to trade and specify the amount and price of the selected title - it is arguable that the selection of the price, amount and title to trade from an investor on a blockchain-based financial platform's website, followed by the signing off of the order through the investor's cryptographic key - which would then trigger the automatic execution from the smart code - would amount to the conclusion of valid financial contracts.

---

[150] Francesco Cocchi, *Il carattere negoziale degli ordini di borsa, Rapporti con il contratto di intermediazione mobiliare e loro autonomia,* in FiloDiritto, 2012: "affermando che attraverso l'esecuzione dell'ordine stesso si pone in essere una fattispecie negoziale, implicitamente *si* (author's italic) conferma la autonoma natura negoziale e non esecutiva dell'ordine, negozio giuridico dotato di propria causa negoziale. Di fatto è in tale momento negoziale che l'acquirente-investitore attua la propria volontà di porre in essere operazioni di investimento, operando la scelta del titolo oggetto di negoziazione, la quantità nonché il prezzo. E' questo l'atto con cui concretamente si manifesta la volontà di procedere alla predisposizione e conclusione di investimenti. Tale decisivo elemento appare idoneo a suffragare la natura negoziale dell'ordine di borsa, il quale appare possedere tutti gli elementi negoziali che gli sono propri e comunque necessari, quali la manifestazione di volontà, la causa negoziale, l'identificazione del bene oggetto del contratto nella sua qualità, quantità e prezzo. E' attraverso la ricostruzione della natura giuridica del contratto quadro quale contratto normativo, diretto a regolamentare i futuri servizi di investimento che si rende possibile quindi un inquadramento delle operazioni di investimento quali atti negoziali autonomi e non quali mere esecuzioni del contratto di intermediazione". https://www.filodiritto.com/articoli/2012/09/il-carattere-negoziale-degli-ordini-di-borsa

[151] Corda is only one of the distributed ledger projects inspired by the blockchain technology being developed by financial institutions. The Australian Security Exchange (ASX) is also experimenting on this technology with an aim to replace CHESS, its clearing and settlement system for cash equities and electronic sub-register of these securities, with distributed ledger technology (DLT). The timeline provided in its most recent consultation paper (https://www.asx.com.au/documents/public-consultations/chess-replacement-new-scope-and-implementation-plan.pdf) foresees that the replacement will go live by 2020.
As a matter of fact, in the Goldman Sachs Group's 2016 *Profiles in Innovation: Blockchain, Putting Theory into Practice,* the post-trade lifecycle of financial transactions is considered to be the most fertile ground for the application of blockchain technology, which could dramatically improve the clearing and settling of trades by reducing/eliminating trade errors and costs given to manual intervention, shortening the settlement times, etc. For a complete overview on the benefits of blockchain technology applied to cash equity trading see here: https://msenterprise.global.ssl.fastly.net/wordpress/2017/07/Goldman-Sachs-Blockchain-putting-theory-to-practice.pdf

Before entering into single smart orders, however, investors/clients would still need to conclude the written master agreement with their broker and a series of pre-contractual information duties lie on the latter in favour of investors. Both fulfillments can be complied with by blockchain-based brokers, since it can be made one of the conditions of the smart codes available on the platform that a written electronic copy of the master agreement and any electronic forms pertaining to pre-contractual information for investor protection are digitally signed and their hash is saved on the blockchain before any smart orders can successfully be entered into.

Furthermore, in a blockchain-based master agreement, the parties may agree that the conclusion and execution of financial orders is remitted to smart codes, making use of the contractual freedom as to the form of financial orders recognised to the parties of a financial relation by prevailing case law[152].

Nevertheless, conflicting opinions as to whether or not the form of financial orders falls into the parties' contractual freedom have arisen from the same case law supporting the thesis of the autonomous contractual force of financial orders, from which one might argue that the their validity is also subject to the written form requirement prescribed by article 23, T.U.F. for master agreements[153].

The implications of such a debate on the validity of single smart orders are, however, limited. In fact, it shouldn't be forgotten that in order for smart contracts to be concluded - and automatically executed - a qualified electronic signature of the executing user must be provided, so that the agreement may be considered as per article 20, Digital Administration Code to be equivalent of an agreement in written form with handwritten signatures. As to any concerns regarding the identifiability of blockchain users through their cryptographic signatures, it is worth mentioning that private/permissioned blockchains the likes of those being built by financial institutions are developing specific ID mechanisms aiming at bypassing the issue but these mechanisms would require specific legislation to be valid.

So far, the analysis has been focussed around the legal status of smart orders concluded on private/ permissioned financial blockchains. The reason for this approach lies in the fact that such tools are likely to

---

[152] See Civil Supreme Court, n. 28432/2011: "E' perciò corretto il principio di diritto al quale la corte d'appello si è attenuta: che, cioè, la forma scritta è richiesta per la validità del c.d. contratto-quadro col quale l'intermediario si obbliga a prestare il servizio di negoziazione di strumenti finanziari in favore del cliente, ma non anche per i singoli ordini che, in base a tale contratto, vengano poi impartiti dal cliente all'intermediario medesimo, la cui validità non è soggetta a requisiti di forma."

[153] See Ravenna Civil Court, n. 1885/2009: "mentre la legge n. 1/91 richiedeva la forma scritta ma faceva più espresso riferimento al contratto quadro, il d.lgs. n. 415/1996 prima e ora l'art. 23 T.U.F. facendo riferimento ai contratti relativi ai servizi di investimento utilizzano l'espressione che seppur non univoca, testimonia l'intenzione del legislatore di fornire maggiore tutela anche per quanto riguarda i singoli ordini di borsa", from which the judge deduced that article 23, T.U.F. " non autorizza una lettura restrittiva della norma, [...] dato che anche i singoli ordini di negoziazione danno luogo alla formazione di contratti e che questi contratti (al pari del contratto quadro) hanno per oggetto la prestazione di servizi di investimento"

become an essential part of our daily institutional trading activity in the near future, and a serious discussion with regards to their juridical nature and conditions for implementation is highly needed.

At the same time, however, it shouldn't be neglected that the very same notion of blockchain and its earliest implementations came about precisely with the aim to dismantle financial institutions' monopoly over the allocation and movement of value in favour of individuals' enhanced autonomy in doing so without the need of any trusted intermediary, which makes the development of a private blockchain developed by a financial institution a contradiction in terms. With this in mind, a closing remark must be made with regard to the increasing amount of smart cryptocurrency orders concluded on public blockchain-based exchange platforms everyday - whose trading venue is estimated in their millions[154] - in a completely unregulated manner.

Blockchain-based exchange platforms recall the mechanism of forex exchanges inasmuch as they allow investors (mainly private parties transacting on the blockchain) to set up the price and amount of the cryptocurrency they intend to buy or sell on the exchange's website, and having a code automatically executing the order as soon as the market price hits the one targeted. This use case of smart contracts falls into the increasingly wide-spread practice of Direct Market Access (DMA) investing, through which investment companies and other private traders (also referred to as "buy side") wishing to trade in financial instruments can do so by interacting directly with the order book of an exchange without having to pass the order over to brokers for execution.

In such a scenario, with investors trading under their own responsibility, the need for a preceding master agreement setting out the terms of the investor - broker financial relation comes less, and the smart code may be considered to be the only valid agreement upon which the trade is concluded.

It would be advisable, however, that blockchain-based exchange platforms provided their users with all the necessary information regarding the conclusion of the smart orders and their consequences, which could be solved by having a preliminary written version of the terms and conditions of the trading taking place on the platform digitally signed by each user when signing up to the platform. There are several implications and risks related to the existence of an unregulated multi-million digital asset trading on public blockchains in terms of investor protection, taxation, money laundering - to name but a few -, some of which have started being addressed by our legislator[155].

---

[154] Camila Russo, *Crypto Exchanges Are Raking in Billions of Dollars,* Bloomberg, 2018: https://www.bloomberg.com/news/articles/2018-03-05/crypto-exchanges-raking-in-billions-emerge-as-kings-of-coins

[155] As far as taxation is concerned, see Agenzia delle Entrate, Risoluzione Ministeriale n. 72 E, 2016: https://www.finaria.it/pdf/bitcoin-tasse-agenzia-entrate.pdf . As to anti-money laundering regulation, see d. lgs. n. 90/2017 (http://www.gazzettaufficiale.it/eli/id/2017/06/19/17G00104/sg) enforcing the Fourth Anti-Money Laundering Directive (EU) 2015/849 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2015_141_R_0003&from=ES)

It is desirable that the regulation of such a phenomenon, however, will be based on the sensible consideration of the potential benefits of this technology, rather than on an indiscriminate censure against it, which would most likely result in the blockading of what could be a great chance for innovation.

CHAPTER 3

Operative Issues Rising from the Use of Smart Contracts

1. Identity problem on the blockchain:

One of the criticisms most frequently levied at the blockchain and smart contracts is its alleged anonymity. A variety of commentators have referenced this as its primary and most irremediable weakness, claiming its anonymity leads to it being "untraceable" and thus a safe haven for criminals and other unsavoury characters. Rightly or wrongly, bitcoin has long been associated to black markets, money laundry and criminality.[156]

This weakness is also considered to have serious repercussions for smart contracts. After all, how can one make a legally binding contract between anonymous parties? Under Italian civil law, only a natural or a legal person may enter into a contractual relationship, provided it has the required legal capacity to do so (according to article 2, Civil Code, minors do not have the legal capacity to enter into most contracts), while the legality of some contracts is contingent on the fulfilment of additional criteria. For instance, the legality of a contract for the sale of an alcoholic beverage is contingent on the purchaser being of legal consumption age. A contract for the sale of a fire arm is contingent on the purchaser being located in a jurisdiction in which this purchase is legal.

Other commentators worry about how to track down parties to an illegal smart contract or a smart contract which malfunctioned in a certain way either due to hacking or other malpractice (an example of which is the infamous DAO hack mentioned in Section 3 on liability of blockchain users). In such cases, if a dispute arose, how would aggrieved participants to a public blockchain identify the other party to a smart contract to legally proceed against them? It is likely that courts will not regard smart contracts hosted on public blockchains as having legally binding effect if identification of their contracting parties is simply precluded[157]. Anonymity, combined with the automatic execution of smart contracts and the immutability of the results they produce, has led some to argue that they are just unsafe and illegal tools.[158]

1.a. Pseudonymity, not anonymity:

---

[156] S. Foley, J. R. Karlsen, T. J. Putnins, *Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?*, January 2018, Available on SSRN: https://poseidon01.ssrn.com/delivery.php?ID=200072070066112000020125018030100006059017001061057056022127074122003117070090104098100005023023018037116127065002004118121096015000017021052107089094117075070122001082062118085086112117078009028091000074064069114006115064116094094000073066021116090&EXT=pdf

[157] R3 and Norton Rose Fulbright White Paper, see note 23

[158] P. Ford, *Bitcoin is Ridiculous. Blockchain is Dangerous*, March, 2018, Bloomberg Businessweek: https://www.bloomberg.com/news/features/2018-03-09/bitcoin-is-ridiculous-blockchain-is-dangerous-paul-ford

However, claiming that blockchain and smart contracts are anonymous is to misunderstand and/or misrepresent the reality of how the technology works. Indeed, anonymity implies that a person's identification is completely precluded (i.e. paying for goods in cash) whereas pseudonymity means that although a person is not identifiable but his or her real name, such identification is made possible by acquiring additional information about that person (i.e. an online alias or an account number at a bank).[159] Blockchain is actually much closer to the latter, as people's identities and all transactions associated to them are tied to verifiable and auditable public ID's present on a public ledger.

Rather than making criminal behaviour easier, many argue this actually makes it more difficult as it simplifies law enforcement's job by ensuring money is always traceable through various public IDs. This is the opinion shared by Jason Weinstein, a partner with Steptoe and Johnson LLP, who also served a term as the deputy assistant attorney general in the US Department of Justice where he was in charge of matters related to cybercrime and organised crime. As he says: "Actually, the bitcoin presents a unique challenge, meaning it actually provides some advantages as far as attribution is concerned. This means that it is not anonymous. In fact, it is rather pseudonymous. This means that the bitcoin address of a user is similar to that of an account number. Therefore, it is possible to connect the user to an address and trace all the transactions".[160] Weinstein further explains this by stating that in order to buy or sell cryptocurrencies into FIAT, users must interact with an exchange or e-wallet. However, these services are legally obligated to keep a record of customer information, much like a bank. As such, law enforcement can obtain user information by means of a subpoena or other lawful process. Thus, the "attribution advantage offered by bitcoin is scalability, traceability and the blockchain's permanence".

However, this pseudonymity still doesn't address the criticism of smart contracts. After all, you can't extract age or jurisdiction from a public ID, and while you can trace down a public ID's identity, this is still a costly and time-consuming process.

1.b. Decentralised identity solutions:

This is where decentralised identity solutions come in. Decentralised identity solutions allow users for "self sovereign identities". In order to understand this concept, it's important to first give an overview of the current status quo. Right now our identities in the form of our personal data are shared all over a variety of different companies' databases. Whenever we have to identify ourselves, we're forced to present a variety of

---

[159] For a definition of anonymity and pseudonymity provided by Opinion 05/2014, Article 29 Working Party - which still applies under the European General Data Protection Regulation 2016/679 (GDPR) - see the following Section on the issues arising from the application of data protection law on blockchain projects

[160] See a report of Jason Weinstein's opinion on the potential of bitcoin for enforcement agencies here: https://totalbitcoin.org/bitcoin-is-not-really-anonymous-but-pseudonymous/

information to prove who we say we are, whether that's to register for an online service, check-in at a hotel or even prove we're old enough to buy cigarettes. These companies and institutions possess permanent access to our data and while they promise not to share it with others, they often break this promise[161] and even when they don't the number of high-profile hacks over the last few years is conclusive proof that our personal data is not safe.[162]

A self-sovereign, decentralised identity solution allows users to have complete ownership and control of their identity and personal data while making cryptographically verifiable claims or attestations about facts or attributes related to their identity.[163] This means that a user can choose to provide certain information about him/herself to a third-party (such as a government institution or company) in the form of a cryptographic proof, without giving the third-party access or ownership of the data itself. Crucially, these proofs can be shared and stored privately, thus preserving the principle of privacy that is characteristic of self-sovereign identity. Indeed, all data is stored only on the users' device, with only a hash proving that the data is verified and untampered being stored on the blockchain.

For the purposes of smart contracts, these decentralised identity solutions allow contracts to confirm certain facts about people without having to know the person's identity. For instance, Civic, a decentralised identity provider, has recently partnered with Anheuser-Busch Inbev to dispense beer from a Blockchain-enabled vending machine in America, using the app to verify the purchaser is over 21-year-old drinking age.[164] Purchasers simply scan a QR code with the Civic app which verifies that the person is over the legal drinking age and dispenses a 12oz can of Budweiser.[165] All this is done anonymously, because Civic's own systems have already verified their users' personal details, including age. Importantly, Civic is not storing this data on its own database as this would simply pose another centralised risk. Rather, all data is stored only on the users' device and a hash of the data proving its immutability is stored on the blockchain. Also importantly, Civic is not acting as a centralised digital identity system "vouching" for that user's age (since Civic itself doesn't have access to this information). Rather, Civic is issuing a cryptographic proof showing the user is over 21 that is then confirmed by the vending machine in a smart contract.

---

[161] K. Schwab, *How Widely Do Companies Share User Data? Here's A Chilling Glimpse,* January, 2018, CO. DESIGN: https://www.fastcodesign.com/90157501/how-widely-do-companies-share-user-data-heres-a-chilling-glimpse

[162] For an overview of the magnitude of the issue, see this non-exhaustive list of data breaches compiled on Wikipedia: https://en.wikipedia.org/wiki/List_of_data_breaches

[163] C. A. Bruguera, *The Decentralised Identity Economy,* April, 2018, Medium: https://blog.selfkey.org/the-decentralized-identity-economy-f3dbfc9a3c3c

[164] T. Shapshak, *Now You Can Buy Beer From An Age-Verifying Blockchain Vending* Machine, May, 2018, Forbes: https://www.forbes.com/sites/tobyshapshak/2018/05/15/now-you-can-buy-beer-from-an-age-verifying-blockchain-vending-machine/2/#da76a960e63e

[165] Ibid.

Civic is only one of many projects working on decentralised identity. There are others like Uport[166] (focussing on credentials) and Selfkey[167] (focussing on KYC information). Together, these decentralised identity systems will allow smart contracts to confirm any legally required fact about a user without the need to expose a users' identity.

In future, these identity protocols will possibly be made mandatory so that every user transacting on a public blockchain will be forced to preliminarily verify his or her identity in order to validly enter into smart contracts.

[166] C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, M. Sena, *Uport: A Platform for Self-Sovereign Identity*, October, 2016 (draft version): http://blockchainlab.com/pdf/uPort_whitepaper_DRAFT20161020.pdf

[167] See Selfkey white paper here: https://selfkey.org/wp-content/uploads/2017/11/selfkey-whitepaper-en.pdf

2. General Data Protection Regulation (GDPR) and blockchain technology: an unresolvable conflict?

Since May, 25th, 2018, the EU's new General Data Protection Regulation ("GDPR")[168] is applicable in all Member States, including the UK, whose government has confirmed its intention to adopt it notwithstanding the national decision to leave the EU[169].

The aim of the new item of legislation is to provide all European citizens with the highest level of protection from privacy and data breaches in an increasingly data-driven world, where the regulatory policies of the 1995 Directive have proven to fall short[170].

Given the increased enforcement rules established by the GDPR - fines of up to 20 million EUR or "4% of the total worldwide annual turnover of the preceding financial year, whichever is higher"[171] - it comes as no surprise that compliance with the new regulatory framework is on top of any firm's agenda, including those in the blockchain space, which makes an analysis of blockchain projects' conformity with the new data protection standards and rules of paramount importance.

Arguably the main change brought by the new data privacy regulation relates to the expanded jurisdiction of the GDPR, which applies to all companies, organisations and individuals processing or controlling personal data in the EU, regardless of whether the processing takes place in the Union[172], and processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union for business ("offering goods or services") or behaviour monitoring ("as their behaviour takes place in the Union") purposes[173]. On the basis of the so-called "household exception", data processed by individuals for purely personal reasons or within non-professional, non-commercial activities are not subjected to the data protection law. However, the rules do apply when individuals process personal data outside the personal sphere, for socio-cultural or financial activities[174].

Such a regulatory setting is hardly adaptable to blockchains, particularly open and public ones. In fact, in such decentralised, cross-border systems with multiple participants located all around the world, it is highly

---

[168] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). See full text here: https://gdpr-info.eu/

[169] Data Protection Act 2018, which updates UK's data protection law and implements the GDPR. See full text here: http://www.legislation.gov.uk/ukpga/2018/12/enacted

[170] GDPR Key Changes, in: https://www.eugdpr.org/key-changes.html

[171] Article 83, (5), GDPR. General conditions for imposing administrative fines.

[172] Article 3, (1), GDPR. Territorial Scope.

[173] Article 3, (2). Territorial Scope.

[174] *What does the General Data Protection Regulation (GDPR) govern?:* https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en

likely to find data controllers or processors with no establishment in the EU nor targeting EU residents next to some participants falling under the material or territorial scope of application of the GDPR. As a consequence, the application of GDPR will likely have to be assessed on a transaction by transaction basis and European data protection rules will possibly apply to blockchain-based transactions that have little or no connection to Europe[175].

In order to assess the relationship between blockchains and data protection law, it is necessary to analyse the definitions provided by the GDPR.

First, the GDPR applies to "personal data", or "any information relating to an identified of identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one to more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

Moreover, recital 26, GDPR specifies that pseudonymised personal data "which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person", thus fitting under the GDPR's scope of application. In particular, in evaluating whether identification through pseudonymised data is possible, account should be taken of all "the means reasonably likely to be used" and "of all objective factors, such as the costs of and the amount of time required for identification".

Only anonymised data are not subjected to data protection law, meaning "information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable"[176].

Consequently, in order to determine whether data protection rules apply to blockchain technology, we need to establish whether personal, pseuodonymised or anonymised data processing takes place on it.

On public blockchains, users transact under their public keys. Although such keys are encrypted, so that no-one viewing the blockchain is able to directly identify the individual or corporation represented by them, their re-use allows to single out the authors of given transactions. In fact, on public blockchains such as Bitcoin, having visible keys is made necessary by the need to prevent double-spending problems by tracking all transactions and making sure they are attributed to the correct people. When public keys are publicly-

---

[175] Hogan Lovells, *A guide to blockchain and data protection*, September 2017: https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf

[176] See Recital 26, GDPR. Not applicable to anonymous data (unofficial title description).
In Opinion 05/2014, the Article 29 Working Party (Data Protection Working Party established by Article 29 of Directive 95/46/EC) - providing the EU Commission with independent advice on data protection matters and helping in the development of harmonised data protection policies in the EU - stated that "anonymisation results from processing personal data in order to irreversibly prevent identification."

available, it could be possible to attain additional information making users' identification possible, for example through their IP addresses or connections to websites. As a consequence, public keys are likely to qualify as personal data on most public blockchains, thus being subjected to the GDPR's rules.
Technological solutions allowing individuals to transact on private and public blockchains without making their public keys visible are being developed. One of them is currently used by Hyperledger Fabric[177], which provides any core private key with a new public "transaction" key for each transaction, so that the same user can transact under a series of different public keys without ever being singled out by the rest of the network. The implementation of such a solution on public blockchains is quite controversial, since it would require the introduction of a key issuing authority, most likely a centralised entity, which seems to contrast with that type of technological setting.
As far as hashing is concerned - the mathematically-irreversible process through which any set of data is turned into a fixed-length number string representing the data's unique "fingerprint" -, its classification as pseudonymised rather than anonymised data has been confirmed by Opinion 05/2014, Article 29 Working Party. According to the working group, any hashes that permit the "linkability" of records to individuals (IDs, phone numbers, medial records, etc.) constitute personal data. On the other hand, hashes representing bill of ladings, for example, would not be considered personal data given that bill of ladings, or information alike, cannot be linked to any individuals.
Last but not least, encryption of data - typical of public and private blockchain - is not deemed to be an anonymisation technique, with the consequence that encrypted data also classifies as personal data and falls under the application of the GDPR. In fact, if enough effort is put into it by experts or someone holds the key to decryption, encrypted data can still be traced back to a person, thus making his or her identification possible.
From the classification of public keys, hashing and encryption as personal data, it follows that existing public and private blockchains will have to come up with alternative solutions relating to data storage and transmission soon if they intend to operate compatibly with the GDPR's provisions and not be subjected to the above-mentioned penalties.
Another challenging aspect relating to blockchain projects' compliance with the GDPR lies in the identification of the parties operating on the distributed network as data controllers or data processors as a preliminary step to verifying compliance with the legal obligations directed to them.
Data controllers are defined by article 4, (7) as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (…)".

---

[177] To know more about Hyperledger Fabric, see: https://www.hyperledger.org/projects/fabric

Their main responsibility is the implementation of appropriate technical and organisational measures that ensure and are able to demonstrate that processing is performed in accordance with the GDPR[178], as well as adopting - both when determining the means for processing and when processing - technical and organisational measures that effectively implement data-protection principles, such as data minimisation, which aims at ensuring that only personal data which are necessary for each specific purpose of the processing are processed[179].

According to article 4, (2) qualify as data processors those same subjects ("natural or legal person, etc.") carrying out "any operation or set of operations (…) performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction". Such activities shall be governed by a binding contract between the processor and the controller setting out the subject-matter, duration, nature and purpose of the processing, together with the type of personal data and categories of data subjects and the obligations and rights of the controller[180].

On this basis, the relation between the GDPR and public, open blockchains seems problematic, if not unreconcilable. In fact, in a peer-to-peer network environment with no central authority or system administrator, every individual uploading data on the blockchain qualifies as data controller of his own data, with the nodes also qualifying as data processors for others' data. In such a scenario, ensuring every nodes' compliance with their responsibilities under GDPR is not an easy task, and the conclusion of the binding contract between data processor and controller required by article 28, (3) is made difficult by the fact that for each transaction, every data controller would need to enter into a smart agreement with the owner of every node in the blockchain.

On the other hand, permissioned blockchains may be designed to meet GDPR's applicable requirements by introducing governance agreements defining the roles of the nodes operating on the network and their responsibilities as to data protection. In such a scenario, the organisation setting up the blockchain would qualify as the data controller, with the consequence that it would be its responsibility to guarantee compliance with the GDPR and to define the terms of data processing in smart contracts concluded only with the network's participants classifying as data processors.

---

[178] Article 24, (1), GDPR. Responsibility of the controller.

[179] Article 25, (1), (2). Data protection by design and by default. The so-called "privacy by design" approach is one of the main innovations introduced by the GDPR. Although the concept has existed for years, it has now been turned into an applicable legal requirement under the GDPR. According to such an approach, data protection techniques shall be included from the onset of the system's designing, rather than being added to it.

[180] Article 28, (3), GDPR. Processor.

The reconciliation between the GDPR and blockchain technology is made even harder when we consider the new sets of rights of the data subjects listed in Chapter 3, GDPR. In particular, EU citizens have been recognised the right of access to their data[181], right to rectification[182] and a so-called "right to erasure"[183]. These two last provisions, in particular, create the most friction with blockchain technology architecture, which is characterised by the immutability feature described in Part 1, from which it follows that any data added to the blockchain will inevitably become part of a publicly-available, incorruptible, distributed ledger. Mere encryption of data stored on blockchains is not enough to meet the requirements of the right to erasure. In fact, even if by destroying the data's encryption key such data become inaccessible, the right to erasure requires the complete erasure of the data from the network rather than just its becoming inaccessible[184]. Several workarounds have been put forward to resolve the conflict. Recent experiments both on public and permissioned blockchains introduce "off-chain" mechanisms which store the personal data separately on another system with restricted access control, while a reference to this data in the form of its hash is stored on the blockchain[185]. The main benefit of such an approach is that it is 100% GDPR compliant, since the data can be completely erased in the off-chain storage, with the consequence that its hash on the blockchain would become completely useless as it does not refer to any existing data.

At the same time, however, off-chain storage highly reduces the benefits typical of blockchain systems, namely transparency - once the data is stored off-chain, data subjects cannot be completely sure as to whom is accessing them -, clarity as to data-ownership and administration - while only the data-owner has the encryption key to access and administer his own data stored on the blockchain, once that data is stored off-chain the question as to who owns the off-chain system arises. Last but not least, the introduction of off-

---

[181] Article 15, GDPR. Right of access by the data subject: "right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data" and a series of information relating to the personal data.

[182] Article 16, GDPR. Right to rectification: "right to obtain from the controller without undue delay the rectification of inaccurate personal data (…). The right to have incomplete personal data completed, including by means of providing a supplementary statement".

[183] Article 17, GDPR. Right to erasure ("right to be forgotten"): "right to obtain from the controller the erasure of personal data concerning him or her without undue delay" when one of the conditions set out in the article applies, in particular when the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed; when the individual withdraws consent or he or she objects to the processing without any overriding legitimate interest for continuing the processing; when the personal data was unlawfully processed; when the personal data has to be erased to comply with a legal obligation; when the personal data is processed in relation to the offer of information society services to a child.

[184] LegalThings One, *LegalThings One: Blockchain & GDPR made possible,* May, 2018, Medium: https://medium.com/legalthingsone/legalthings-one-blockchain-gdpr-made-possible-68a5ce09e7ca

[185] Andries Van Humbeeck, *The Blockchain-GDPR Paradox,* November, 2017, Medium: https://medium.com/wearetheledger/the-blockchain-gdpr-paradox-fc51e663d047

chain storage linked to blockchains adds complexity to the system as a whole, which increases the risk of unintended errors.

All in all, several issues arise once blockchain projects are analysed through the lens of the new GDPR. Hopefully, as time goes by the European privacy regulator will provide specific guidance on how data protection law should be applied to distributed ledger technology.

3. Liability for software breach or bugs on public blockchains

One of the main questions arising from the use of blockchain technology and smart coding as a contracting tool concerns the regulation of cases of software non or incomplete performance or security breach resulting in a damage to contracting or third parties, especially with respect to who will bear responsibility for such a damage in a distributed ledger scheme.

Nevertheless, the relevance of such a question seems to be completely overlooked by the most enthusiastic supporters of the technology, some of whom still envisage a technological "oasis" exempt from what is perceived as the unnecessary burden of legal provisions. The approach embraced by these "technological utopians" is summed up in the leitmotif that "Code is law"[186]: while law controls human behaviour, coding will design and structure a separate space - the cyberspace - hosting machine-based interactions, within which a core set of values will be established by engineers, or the "governors" of such a space. This "Code is law" defence would possibly be raised by any defendants in a lawsuit for damage caused by security breach or software malfunctioning, in the belief that everything and only that which is permitted by the code - including malevolent attacks taking advantage of unknown weaknesses of the code itself - should be considered as "legal".

Certainly, there is a long list of reasons why such an argument would not be accepted by any judge, starting from the basic public law notion of the "rule of law", from which it follows that legal provisions shall only be validly elaborated by the formal law making bodies of a specific legal system which have been vested with such a power: as long as the constitutional order of a given system is not overturned by machines and softwares completely taking over, code is not law. Another reason against the adoption of a "code is law" perspective lies in the fact that it is simply inconvenient to do so: the measure of future success of public blockchain technology and smart coding also depends on whether or not users will be provided with appropriate legal protection if anything goes wrong, because at some point, something will go wrong. In fact, vulnerabilities in softwares are seen as unavoidable even by developers themselves, according to whom "software today remains, in many ways, far less reliable and more prone to bugs than in the past."[187].

If one takes a more facts-based stand, one cannot ignore that reality has already proven that things can go really wrong on public blockchains and without adequate legal regulation, users will pay the consequence of

---

[186] See L. Lessig, note 19: "[t]he code of cyberspace—whether the Internet, or a net within the Internet— defines that space. It constitutes that space. And as with any constitution, it builds within itself a set of values and possibilities that governs life there … And the design of code is something that people are doing. Engineers make the choices about how the world will be. Engineers in this sense are governors".

[187] D.E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1022 (2014) (quoting Claire Le Goues et al., The Case for Software Evolution, 18 PROC. FSE/SDP WORKSHOP 205, 205 (2010))

such malfunctions. Here, reference is made to the now infamous DAO attack[188]. On May, 2016, an open source software developed by the Slock.it team was built on the Ethereum blockchain which took the form of a very complex smart contract. The aim of the Decentralised Autonomous Organisation was to operate like a venture capital fund for crypto and decentralise space without any centralised entity controlling the funds and releasing them, nor any legal entity operating as a liability shield of investors' assets. By sending Ether to the DAO wallet address, the investors would get DAO tokens in exchange and be entitled to vote on white-listed investment proposals, as well as share the profits generated by such investments. Expectations on the success of the DAO were really high: the moment had come for the Ethereum blockchain to prove its ability to fulfil the promise of completely automised business conduction based on a decentralised governance structure. Investors' response to the project was overwhelming, with more than $250 million worth of Ether kept in the DAO wallet address at some point. Everything was going smoothly, with proposals being created and voted by DAO's investors, until June, 18th, 2016, when members of the Ethereum community realised that the ETH balance of the DAO's smart contract had gone down, with $70 million worth of Ether at that time having disappeared. Later on, it was found that the hacker had taken advantage of bugs in the code implemented on the Ethereum blockchain to withdraw funds to his or her wallet. At that point, the Ethereum core developers took over presenting different proposals to be voted by the entire community on how to deal with the consequences of the wrongdoing: an initial "soft" fork solution was put forward, according to which the basic Ethereum code would be modified in order to "freeze" the stolen DAO assets and not let the hacker transact them on the Ethereum blockchain - which, however, did not provide for the restitution of the embezzled funds to the investors. The hacker itself responded to such a proposal with an open letter, in which he or she threatened to take legal action against whoever invalidate his work, precisely on the basis of the "code is law" defence: the smart contract is its only arbiter and nothing outside what is written in the piece of code - even when such a piece of code contains unknown, exploited bugs - can be held against it. Ultimately, a "hard" fork was voted: the core developers of Ethereum unilaterally made the decision to create a new version of the Ethereum blockchain, Ethereum Classic, on which the effects of the hack were eliminated by refunding the DAO token holders of the stolen funds. Not all Ethereum users decided to update the new version of the software, and the two Ethereum blockchains now coexist, with the original one not having returned the stolen funds on the basis of the sacred assumption of the blockchain's immutability. Before moving on to outline the legal discussion as to liability for software attacks or bugs that this event spawned, it is important to understand that the Ethereum blockchain is not to be deemed responsible for the embezzlement of the DAO funds, and the question of its suitability to host complex smart contracts allowing for enhanced automation in business conduction should not be

undermined by the DAO: doing so would amount to blaming the whole Internet for the malfunctioning of a single website. At the same time, however, increased attention has been focussed around the role of blockchain developers and miners in the development and running of public blockchains as a consequence of this episode, which leads back to the initial question on the applicable liability scheme for software breaches and bugs. To this purpose, some preliminary observations are necessary: first, in the absence of any blockchain legislation regulating tort law matters, any solutions put forward by legal scholars and operators will be based on the application of a given system's foundational principles, starting from the generally-accepted one that "artificial responsibility" of machines is not legally relevant: the parties to a smart contracts will always be deemed to be humans and identified in the person or group of persons exercising control over the non-human electronic agent by virtue of ownership, management rights, or other linking factors[189]. Furthermore, the question of legal liability schemes on blockchains has a different scope on private and public blockchains: while the former are provided with a sometimes highly-structured governance model within which nodes have clearly distinguished roles with some of them bearing internal and external liability, the same is not true for public blockchains like Bitcoin and Ethereum, where there is no common knowledge of who are the entities involved in the development and running of the underlying protocol. What is true for both blockchain models, however, is that the current lack of shared legal standards applying to distributed ledger technology's processes and services makes it difficult to identify a duty of care lying on blockchain core developers from whose breach a liability in negligence arises.

On this basis, interesting solutions to the liability problem on public blockchains have been put forward by professor Angela Walch[190], on one side, and a Law research group from University of New South Wales[191] . According to the former, an analysis of the powers exercised by Ethereum core developers and miners as a consequence of the DAO attack reveals the legal characterisation that should be given to such users, namely that of fiduciaries of Ethereum holders. Indeed, they were responsible for substantial governance and technical decisions with huge economic impact on the whole community. From the recognition of their fiduciary role, a series of duties would follow which could positively reflect on the general level of performance on public blockchains, in particular: a duty of care, or to act with the appropriate competence - according to the general provision of article 1176, Civil Code -, a duty of loyalty, or to act to protect and fulfil the interests of those they serve over their own specific interest - stated with reference to employees by

---

[189] Kolber, Adam J., *Not-So-Smart Blockchain Contracts and Artificial Responsibility,* May 28, 2018, Stanford Technology Law Review, 2018. Available at SSRN: https://ssrn.com/abstract=3186254

[190] A. Walch, *Call Blockchain Developers What They Are: Fiduciaries*, August, 2016, American Banker: https://www.americanbanker.com/opinion/call-blockchain-developers-what-they-are-fiduciaries

[191] D. A. Zetzsche, Ross P. Buckley, D. W. Arner, *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*, University of New South Wales Law Research Series, 2017: http://www5.austlii.edu.au/au/journals/UNSWLRS/2017/52.pdf

article 2105, Civil Code. The exact content of such duties is determined once the nature of the fiduciary relation is defined: for example, should miners and developers be seen as partners in a distributed company, thus carrying enhanced care duties, as provided for by article 2392, Civil Code, the specific norm ruling on liability of company managers? Response to such questions will come from new legal provisions and national courts' rulings.

The University of New South Wales, however, attempted to foresee such solutions in order to assess the potential liability risks lying on the different groups of users currently involved in distributed ledger schemes. Their research started off by identifying five different groups making up any distributed ledger technology (DLT) scheme, consisting of: (1) the core group of developers, those with technical and governance leadership who are entitled to prompt a "hard" fork; (2) validation nodes; (3) so-called "qualified users" of the DLT like exchanges, miners, etc.; (4) "simple users", or owners of cryptocurrencies; (5) third parties that are indirectly affected by the technology, like counterparts of "simple users".

Moreover, four different sources of liability have been identified, among which one deserves a brief illustration given that it seems to strengthen a point previously made in Part 2, 2.a. of this essay with regards to manifestation of blockchain users' assent to enter into legally binding relations through the completion of the necessary steps needed to set up a cryptocurrency wallet. In fact, the authors identify the existence of a contractual relationship between groups 1-4, on one side, and group 5 on the other can be envisaged, and consider breach of such a relation amounting to contractual liability of the breacher. Interestingly, the research group considered both the core software developers and the validation nodes to be part of a so-called "distributed ledger contract" on the basis of the assumption that the system would not work without them, and regardless of whether or not such members intended to enter into legally binding relations. In fact, the very fact that they voluntarily download the software and make their computers available to the overall functioning of the blockchain amounts to legally consequential conduct, especially given that they know that third parties will rely upon such system. According to general principles of contract law on liability, the existence of a breach of contract depends on the conduct held by the parties considered in the context of the contract terms, which will have to be expressed prior to entering into the agreement. Consequently, the legal suitability of Open Source Software Licenses (OSSL), as it is the case with Bitcoin and Ethereum[192], to limit the developers' liability will have to be assessed by judges, and it would probably fail such a test once our

[192] The typical formulation of Open Source Software License is as followed: "THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE."

national legislation on abusive clauses within C2C and B2C relations is taken into account[193]. The main objection to the statement that DLT relationships give rise to legal rights is based on the idea that public blockchains' users are unknown and the userbase unstable, given that the running of the blockchain depends on who is connected at any given time, from which it should follow that no contractual relationship exists in distributed networks. However, the paper rightfully notices that within complex business structures, too, the identity and roles of participants are not known by all entity's components and that is not a solid basis upon which lack of liability can be argued. According to the study, alternative sources of liability are represented by law of torts - or extra-contractual liability - on the basis of which, even in the absence of a contractual relationship - the causing of a loss or a damage entitles the plaintiff to collect an award from the individual - or group of individuals in case of joint liability - responsible for such a loss or damage. Ultimately, the theory of groups 1-2 representing partners of an unincorporated company coming to existence on the basis of the joint pursuit of a shared economic objective, as it is in the case of the running of a blockchain system.
So far, the liability lying on users involved in the development and running of public blockchains has been considered.

The debate on the role and connected liability of users involved in the blockchain environment has just started, and it is highly recommendable that a serious discussion on the topic is fostered in order to make public blockchains, safer blockchains.

[193] Here reference is made to articles 1341, Civil Code and articles 33, ss. Consumer Code

CONCLUSION

Given the surprisingly high pace with which blockchain technology and smart contracts have been evolving in the recent years, the assessment of the legal status of smart contracts under our legal system is likely to become of large interest for legal practitioners in the near future. In the absence of any legislation or case law on such a topic, this dissertation has attempted to enquire how the general principles of traditional contract law can be applied to smart contracts with a view to establish whether or not they can be deemed to be legally binding agreements under Italian contract law. From such an analysis, it is arguable that smart contracts can meet the essential requirements provided by article 1325, Civil Code referring to the reaching of a mutual binding assent and to the respect of the written form prescribed for specific contracts, thus opening up a path to the recognition of their legally binding force. At the same time, however, this dissertation sustains that the suitability of smart contracts to become a wide-spread contracting tool is contingent upon the degree of collaboration that will be established between technology developers, on one side, and legal practitioners on the other. As a matter of fact, traditional contract law and smart contracting should not be seen as two mutually exclusive systems, but rather as two mutually-beneficial possible solutions to the same problem: easing the creation of valid contractual agreements. While traditional contract law should be open to the possibility of recognising smart contracts as legally binding agreements and focus on solving the - many - legal issues arising from their application, supporters and developers of smart contracts need to admit the undeniable value of the definitions, principles, and solutions elaborated by traditional contract law in its century-long experience. Moreover, the positions of the most enthusiastic supporters of smart contracts - claiming that smart contracts don't need any legal system to exist or that their validity is not dependant upon the provisions of national legislations - should be mitigated by the awareness that national states do have the upper hand as far as the use of blockchain and smart contract is concerned, given that they could potentially adopt drastic measures to retain control over the blockchain environment if they were threatened by its unregulated use. For instance, Internet service providers could be instructed to ban encrypted data, software developers or users of unlawful blockchain institutions could be prosecuted by centralised authority, or hardware manufactures could be required to purposefully break their products when certain encryption techniques are being used[194].

It goes without saying that such an extreme scenario is the least advisable one. The blockchain technology and smart contracts may represent a great chance for innovation for contracting, and the technological and legal fields will have to play an equally important role in the definition of how this is achievable.

Hopefully, this dissertation made a little contribution in this sense.

---

[194] A. Wright, P. De Filippi, see note 79

BIBLIOGRAPHY

BOOKS

U. Chohan, *The Double Spending Problem and Cryptocurrencies. Banking & Insurance Journal.* Social Science Research Network (SSRN)

B. Mihir, Rogaway, Phillip, *Introduction to Modern Cryptography,* 2005

Andreas M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, 2014

Lawrence Lessig, *Code, and Other Laws of Cyberspace,* 1999

André Munro, *State of Nature, Political Theory*, Encyclopaedia Britannica

Thomas Hobbes, *The Leviathan*, 1660

Ian Ward, *Thomas Hobbes and the Nature of Contract*, Studia Leibnitiana, Bd. 25, H. 1, 1993

M. Weber, *Politics as a Vocation*, 1919

Francis Fukuyama, *Trust: Social Virtues and the Creation of Prosperity,* Simon and Schuster, 1996

Evgeny Morozov, *The Net Delusion*, 2011

A. G. Guest, *Anson's Law of Contract,* Twenty-sixth edition

E. Tosi, *Contratto virtuale. Procedimenti formativi e forme tra tipicità e atipicità,* Milano, 2005

E. Tosi, *Diritto privato dell'informatica e di Internet, I beni - I contratti - Le responsabilità*, Milano, 2006

E. Tosi, *Il contratto virtuale: ricostruzione della categoria negoziale,* in *I contratti informatici*, a cura di R. Clarizia, in Rescigno, Gabrielli, *Trattato dei contratti*, Milano, 2007

E. Gabrielli, *Commentario del Codice Civile,* Dei Contratti in Generale, a cura di E. Navaretta e A. Orestano, artt. 1321-1349, UTET Giuridica, 2011

M. Grondona, *Diritto dispositivo contrattuale. Funzioni, usi, problemi*, Giappichelli Editore, 2011

P. Rescigno, *Le due "versioni" del pluralismo*

F. Modugno, P. Carnevale, A. Celotto, C. Colapietro, M. Ruotolo, G. Serges, M. Siclari, F. Rimoli, *Diritto pubblico*, Giappichelli Editore, 2017

R. Sacco, G. De Nova, *Il contratto*, t. I, UTET; 3 edizione, 2004

C. Restivo, *Contributo ad una teoria dell'abuso di diritto*, Milano, Giuffré, 2007

E. Russo, *Il termine del negozio giuridico*, Milano, Giuffre, 1973

A. D'Angelo, *Contratto e operazione economica,* G. Giappichelli, 1992

V. Roppo, *Il contratto*, Giuffré Editore, 2011

F. Durante, *Intermediari finanziari e tutela dei risparmiatori,* Giuffré, Milano, 2009

G. Bersani, *La responsabilità degli intermediari finanziari,* UTET Giuridica,

JOURNALS

Alexander Savelyev, *Contract Law 2.0: «Smart» Contracts As the Beginning of the End of Classic Contract Law,* 2016

Harry Surden, *Computable Contracts,* University of California, Davis, 2012

David Yerman, *Corporate Governance and Blockchain Technology*, NYU Stern School of Business, 2016

Primavera De Filippi, *Legal Framework For Crypto-Ledger Transactions,* 2015

Max Raskin, *The Law and Legality of Smart Contracts,* Georgetown Law and Technology Review 305, 2017

Clack, Bakshi, Braine, *Smart Contract Templates: foundations, design landscape and research directions*, 2016

Isaak I. Dore, *Deconstructing and Reconstructing Hobbes*, Louisiana Law Review, vol. 72, num. 4, 2012

M. Atzori, *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?*, 2015

Francesca Fasullo, *Il Principio di Autonomia Privata e Contrattuale*

A. Cunningham, *Decentralisation, Distrust and Fear of the Body: the Worrying Rise of Crypto-Law*, Scripted, vol. 13, issue 3, Dec. 2016

K. Werbach, *Trust, But Verify: Why the Blockchain Needs the Law,* Berkeley Technology Law Journal, 2016

A. Wright and P. De Filippi, *Decentralized Blockchain and the rise of Lex Cryptographia*, Mar, 2015

T. Gutmann, *Theories of contract and the concept of autonomy*, Preprints and Working Papers of the Centre for Advanced Study in Bioethics, Münster 2013/55

T. Iraklithe, *The Principle of Freedom of Contract*, Pre-Contractual Obligations Legal Review English, EU and US Law, European Scientific Journal February 2017 edition Vol.13, No.4

Ian Grigg, *The Ricardian Contract*, First IEEE International Workshop on Electronic Contracting, 2004,

A. Zelcevic - Duhamel, *La notion d'économie du contrat en droit privé*, in JCP - La Semaine Juridique Edition Générale, 2001, n. 28

E. Gabrielli, *Il contratto e l'operazione economica*, in Riv. dir. civ. 2003, I

E. Gabrielli, *L'operazione economica nella teoria del contratto*, in Riv. trim. dir. proc. civ., 2009

E. Gabrielli, *"Operazione economica" e teoria del contratto, Studi,* Giuffré Editore, 2013

E. Betti, *Teoria generale del negozio giuridico,* Camerino Rist. 1994

E. Betti, *Causa del negozio giuridico,* in *Noviss. Dig. It.* III, Torino 1957

Giovanni B. Ferri, *La cause nella teoria del contratto*, in Ferri e Angelici, *Studi sull'autonomia dei privati*, Torino, 1997

Roppo, *Il contratto*, in *Trattato Iudica e Zatti*, Milano, 2001

G. O. Hernandez, *Magic circle firms double down on legal smart contracts*, Legal Week, 2018

E. Milk, *Formation Online*, 159, in M Fumston and G J Tolhurst, Contract Formation: law and practice, OUP, 2010

A. Cohn, T. West, C. Parker, *Smart After All: Blockchain, Smart Contracts, Parametric Insurance and Smart Energy Grids*, 1 Geo. L. Tech. Rev. 273, 2017

Francesco Cocchi, *Il carattere negoziale degli ordini di borsa, Rapporti con il contratto di intermediazione mobiliare e loro autonomia,* in FiloDiritto, 2012

S. Foley, J. R. Karlsen, T. J. Putnins, *Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?*, January 2018

D.E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1022 (2014)
Kolber, Adam J., *Not-So-Smart Blockchain Contracts and Artificial Responsibility,* May 28, 2018, Stanford Technology Law Review, 2018

D. A. Zetzsche, Ross P. Buckley, D. W. Arner, *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*, University of New South Wales Law Research Series, 2017

LEGISLATION

Italian

Italian Central Bank, Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica, June, 1st, 2016

D. Lgs. September, 6, 2005, n. 206, Codice del consumo

Testo Unico della Finanza (T.U.F.), d. lgs., February, 24, n. 58

CONSOB, Regolamento intermediari, n. 16190/2007.

D. Lgs. April, 9, 2003 n. 70, Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno

D.lgs. March, 7, 2005 n. 82, Codice dell'amministrazione digitale, aggiornato al decreto legislativo 13 Dicembre 2017, n. 217

Law March, 25, 1997 n. 59, Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione normativa

D. P. R. n. 445/2000, Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa

Regio Decreto 16 marzo 1942, n. 262, Codice Civile Italiano aggiornato

Law January, 2, 1991, n.1, Disciplina dell'attività di intermediazione mobiliare e disposizioni sull'organizzazione dei mercati mobiliari

Agenzia delle Entrate, Risoluzione Ministeriale n. 72 E, 2016

D. lgs. May, 25, 2017 n. 90, di attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attivita' criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE e attuazione del regolamento (UE) n. 2015/847

riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il regolamento (CE) n. 1781/2006

European Union and Member States'

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market

Reg. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

French Ordonnance n° 2016-520 of April, 28th, 2016

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

UK Data Protection Act 2018

American

The American Restatement (Second) of the Law of Contracts, 1981

Arizona, House Bill 2417

Vermont, House Bill 868

RULINGS

Italian Constitutional Court, ruling n. 268, June, 30th, 1994

Italian Civil Supreme Court, n. 1508/1948, n. 3891/1969

Italian Civil Supreme Court, ruling n. 23701/2016

Italian Civil Supreme Court, SS. UU., ruling n. 898/2018

Milan Court of first instance, ruling n. 7076/2012

Italian Civil Supreme Court, SS. UU., ruling n. 26724/2007

Venice Court of first instance, ruling n. 606/2007

Ravenna Court of first instance, ruling n. 1885/2009

Cuneo Court of first instance, ruling n. 358/2012

Italian Civil Supreme Court, ruling n. 28432/2011

MISCELLANEOUS

Timothy May, *The Crypto Anarchist Manifesto*, 1998

Eric Hughes, *A Cypherpunk's Manifesto*, 1990

WikiLeaks, The Spy Files

Wei Day, b-money white paper, 1998

Satoshi Nakamoto, B*itcoin: A Peer-to-Peer Electronic Cash System,* 2008

Vitalik Buterin, *Ethereum White Paper: A Next Generation Smart Contract & Decentralised Application Platform*

Gavin Wood, *Ethereum: A Secure Decentralised Generalised Transaction Ledger*

Nick Szabo, *Smart Contracts: Building Blocks for Digital Markets,* 1996

Gary J. Ross, *Why Lawyers Won't Be Replaced By Smart Contracts,* 2017

Nick Szabo, *On The Blockchain and Smart Contracts,* 1996

Josh Stark, *Making Sense Of Blockchain Smart Contracts*, 2016

Nick Szabo, *Smart Contracts: Building Blocks For Digital Markets*, 1996

Josh Stark, *The Two Topics in Law and the Blockchain,* 2016

I. Bogost, *Cryptocurrency Might be a Path to Authoritarianism*, May, 2017, The Atlantic

L. Dormhel, *Why Your Next Judge (Probably) Won't Be A Robot?*, 2013

Scientific Foresight Unit (STOA) of EPRS, European Union, *What If Blockchain Technology Revolutionised Voting?*, 2016

R3 and Norton Rose Fulbright White Paper, *Can Smart Contracts Be Legally Binding Contracts?*, 2016

Declaration on European Partnership on Blockchain

Principles, Definitions and Model Rules of European Private Law, Draft Common Frame of Reference (DCFR) Outline Edition, 2009

Declaration on European Partnership on Blockchain

Grut, *Only 48% of ICOs were successful last year - but startups still managed to raise $5.6 billion,* in Business Insider UK

LegalThings One white paper

Capgemini Consulting Interview, June-July 2016, in *Smart Contracts in Financial Sector: Getting from Hype to Reality,* 2016

Goldman Sachs Group's 2016 *Profiles in Innovation: Blockchain, Putting Theory into Practice*

Camila Russo, *Crypto Exchanges Are Raking in Billions of Dollars,* Bloomberg, 2018

P. Ford, *Bitcoin is Ridiculous. Blockchain is Dangerous*, March, 2018, Bloomberg Businessweek

K. Schwab, *How Widely Do Companies Share User Data? Here's A Chilling Glimpse,* January, 2018, CO. DESIGN

C. A. Bruguera, *The Decentralised Identity Economy,* April, 2018, Medium

T. Shapshak, *Now You Can Buy Beer From An Age-Verifying Blockchain Vending* Machine, May, 2018, Forbes

What does the General Data Protection Regulation (GDPR) govern?

Hogan Lovells, *A guide to blockchain and data protection*, September 2017

LegalThings One, *LegalThings One: Blockchain & GDPR made possible,* May, 2018, Medium

Andries Van Humbeeck, *The Blockchain-GDPR Paradox,* November, 2017, Medium

A. Walch, *Call Blockchain Developers What They Are: Fiduciaries*, August, 2016, American Banker

SITOGRAPHY

MK, Euro Info Correspondence Centre (Belgrade, Serbia), *E-commerce-Factor of Economic Growth*

https://www.theguardian.com/news/series/cambridge-analytica-files

https://en.bitcoin.it/wiki/Irreversible_Transactions

http://www.oraclize.it/

https://cointelegraph.com/explained/blockchain-oracles-explained

http://www.abc.net.au/news/2017-04-12/$2.6-billion-price-tag-on-nsw-land-titles-registry-sale/8439176

https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf

https://eurasianet.org/s/georgia-authorities-use-blockchain-technology-for-developing-land-registry

https://monax.io/explainers/permissioned_blockchains/

https://www.capgemini.com/consulting/wp-content/uploads/sites/30/2017/07/smart-contracts.pdf

http://www.commonaccord.org/

https://azure.microsoft.com/en-us/solutions/blockchain/

https://www.r3.com/

https://livecontracts.io/

https://wavesplatform.com/

https://www.openbazaar.org/

https://www.asx.com.au/documents/public-consultations/chess-replacement-new-scope-and-implementation-plan.pdf

https://msenterprise.global.ssl.fastly.net/wordpress/2017/07/Goldman-Sachs-Blockchain-putting-theory-to-practice.pdf

https://en.wikipedia.org/wiki/List_of_data_breaches

https://www.hyperledger.org/projects/fabric