A legal analysis of the use of blockchain technology for the formation of smart legal contracts*

Giusella Finocchiaro - Chantal Bomprezzi

Abstract

The object of the present work is to provide a legal analysis of the formation of legally binding agreements through blockchain-based smart contracts. Smart contracts are computer codes that are capable of running automatically upon the occurrence of specific conditions and according to pre-specified functions. These codes can be stored and processed on a blockchain and any change is recorded in the blockchain. The expression "smart legal contract" refers to the use of smart contracts in the contractual domain to perform already existing contracts or to express legally binding agreements in the form of lines of computer code. Regarding the latter, researchers question whether blockchain-based smart contracts can be considered legally binding contracts. The study aims at putting in correlation contract requirements with blockchain-based smart contracts. The scope of the analysis is to verify how to interpret the rules on contract formation to make blockchain-based smart contracts fit into contract law.

Summary

Keywords

blockchain - smart contract - contract law - contract formation – e-commerce

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio a doppio cieco.

1. Introduction

Blockchain-based smart contracts are self-executing computer programs stored on a blockchain, which can be used in the contractual domain to perform already existing contracts or to express legally binding agreements in the form of lines of computer code. The basic idea is that impartial computers might replace corruptible humans in conducting their affairs.[1] Blockchain technology might reinforce this idea thanks to its decentralised and immutable nature.

There is an academic debate about the implications of blockchain-based smart contracts on contract law. The main question is whether they can be considered as contracts, taking into account that they are merely lines of code, that the blockchain is an emerging technology, and that there are some legal requirements to form legally binding agreements.

On this point, it has to be evidenced that blockchain-based smart contracts can fit other uses cases apart from the contractual domain, and they do not always have a legal significance. The present work aims at putting in correlation contract requirements with blockchain-based smart contracts. The scope of the analysis is to verify how to interpret the rules on contract formation to make blockchain-based smart contracts fit into contract law. It focuses on the exchange of offer and acceptance, the time of conclusion of the contract, the contractual intention, and the form of the contract.[2]

Two sections deepen the topic of information requirements and acknowledgment of receipt laid down in the Directive 2000/31/CE[3] and Directive 2011/83/UE[4] because they apply before or at the moment of placing an online order, so they concern contract formation.

Since blockchain technology and its applications are a global phenomenon, to make the work both adaptable to multiple jurisdictions and to foster broader discussions, the paper refers to the three most important sets of contract law principles: The Unidroit Principles of International Commercial Contracts (PICC),[5] the Principles of European Contract Law (PECL), [6] and the Draft Common Frame of Reference of Eu-

---

[*] L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio a doppio cieco

[1] E. Mik, *Smart contracts: terminology, technical limitations and real world complexity*, in *Journal of Law, Innovation and Technology*, 9, 2017, 270.

[2] It does not investigate sufficient agreement and indicia of seriousness that do not seem to pose different issues.

[3] 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 (the so called "Directive on electronic commerce").

[4] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (the so called "Consumer Rights Directive").

[5] *Unidroit Principles of International Commercial Contracts*, Rome, 2016.

[6] O. Lando - H. Beale (eds.), *Principles of European Contract Law*, Parts I and II, The Hague - London - Boston, 2000; O. Lando - E. Clive - A. Prüm - R. Zimmermann, *Principles of European Contract Law*, Part III, The Hague - London – Boston, 2003.

ropean Private Law (DFCR).[7] In addition, as the work assesses contracts concluded by electronic means, it also refers to the Model Law on Electronic Commerce (MLEC),[8] the Model Law on Electronic Signatures,[9] and the United Nations Convention on the Use of Electronic Communications in International Contracts.[10]

2. Blockchain-based smart contracts: a technical overview

"Blockchain" is an umbrella term that includes several independent projects. To date, the two prominent blockchain implementations are Bitcoin[11] and Ethereum.[12] The former was designed to handle financial transactions and to be a core asset for a decentralised virtual market where users exchange virtual coins.[13] The latter, on the other hand, has become a flexible tool for handling secure and trustworthy exchanges of information beyond the financial field, including smart contracts.

A smart contract is a collection of code (its functions)[14] and data (its state)[15] that resides on a specific address (or account). The state of the smart contract can change according to the inputs it receives – which call the functions - and the corresponding output –which depends on the instructions provided by the code. Every change of state represents a transaction that is stored in the blockchain. The code is written in a specific computer language. For instance, the language of Ethereum is Solidity. Solidity is a Turing-complete programming language, which means that it can express any computable function. In Ethereum, every transaction is not free of charge but has a cost that depends on the complexity of the smart contract and is expressed in units called "gas".[16] This is due to the computational effort needed to run the contract.[17]

Blockchains are data structures distributed across a network of computers (or nodes).

---

[7] C. von Bar - E. Clive - H. Schulte-Nölke, *Principles, Definitions and Model Rules of European Private Law: Draft Common Frame of Reference (DFCR),* Munich, 2009.

[8] UNCITRAL, *Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998*, New York, 1999.

[9] UNCITRAL, *Model Law on Electronic Signatures with Guide to Enactment 2001*, New York, 2002.

[10] UNCITRAL, *United Nations Convention on the Use of Electronic Communications in International Contracts*, New York, 2007.

[11] www.bitcoin.org. The author of the Bitcoin white paper is Satoshi Nakamoto. See S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System.*

[12] www.ethereum.org. The author of the Ethereum white paper is Vitalik Buterin. See V. Buterin, *Ethereum White Paper: A next-generation smart contract and decentralized application platform.*

[13] On virtual coins, see A. G. Gambino - C. Bomprezzi, *Blockchain e criptovalute*, in G. Finocchiaro - V. Falce (eds.), *Fintech: diritti, concorrenza, regole. Le operazioni di finanziamento tecnologico*, Bologna, 2019, 267 ss.

[14] In computer science, a function is a section of a computer program that works based on inputs (requests, or calls) and produces a corresponding output (result).

[15] In computer science, a state of a computer program corresponds to its actual values or contents.

[16] Every gas unit corresponds to a certain amount of crypto-currencies.

[17] For a detailed description of the functioning of smart contracts in Ethereum, see C. Dannen, *Introducing Ethereum and Solidity – Foundations of Cryptocurrency and Blockchain Programming for Beginners*, New York, 2017.

Users can interact with the blockchain (i.e. read and write transactions) through their user profiles, also called wallets. A software infrastructure supports the blockchain data structure, ensuring that: nodes can join and leave the network, without compromising the global status of the blockchain data structure; nodes can either discard or accept every change in the blockchain.

Blockchains are made up of blocks. Each block contains: (i) a timestamp, recording its creation time, (ii) a nonce, i.e. a numeric value associated to that single block, (iii) the identifier of another block, (iv) a block status among valid, non-valid, and orphan,[18] and finally (v) a sequence of smart contract transactions. A transaction can either be the uploading of a smart contract on the blockchain or the invocation of some operation of the smart contract.

Hash functions identify each block. Hash functions detect tampering activities: by knowing the block bits and the block hash, the hash function of the block bits can be computed, and it can be checked whether the returned value is the same as the original block hash.

Wallets are software applications that hold the pair of keys used to read and write data in the blockchain. Indeed, each user has a pair of keys. The public key acts as a sort of public address. Users use it to send transactions to the owner of the key. The private key has to be kept secret because it is used to add transactions. The combination of private and public keys is called asymmetric cryptography.[19]

The peculiarity of blockchain technology, as revealed by its name, is that the records of the transactions are grouped to form a block, and the blocks are linked to form a chain. Since every block in the blockchain refers to a previously existing block through its hash, the blockchain is considered immutable. Indeed, any unauthorised change will be immediately visible, because it would cause a modification of the hash and the linked ones.[20]

Usually, blockchains can be permissionless or permissioned. Differences have regard to the different types of permission granted to network participants. Namely, there is the permission to write (i.e. to generate new transactions) and commit (i.e. to update the state of the ledger and add new blocks).[21] In permissionless blockchains, anyone can become a user and write transactions without pre-identification. Any computer can be a node in the network.[22] Furthermore, everyone can add new blocks and update the ledger. In permissioned blockchains, only pre-selected participants can trans-

[18] A block is valid when the network accepts to add it to the blockchain. In the opposite case, the block is not valid. Instead, a block is orphan when the majority of the network initially accepts it but later rejects it in case a longer blockchain does not include that specific block.

[19] In asymmetric cryptography, the key that is used to encrypt the data differs from the key used to decrypt such data. So, asymmetric cryptography is more secure than symmetric cryptography, because it is not necessary to share the same key.

[20] For an overview of the functioning of blockchain technology, see Z. Zheng - S. Xie - H. Dai - X. Chen - H. Wang, *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*, proceedings of the 2017 IEEE 6th International Congress on Big Data, Honolulu, 25-30 June 2017. For more details, see I. Bashir, *Mastering Blockchain*, Birmingham – Mumbai, 2018.

[21] G. Hileman - M. Rauchs, *2017 Global Blockchain Benchmarking Study*, in *Social Science Research Network (SSRN)*, 22 September 2017, 20.

[22] Permissionless ledgers usually rely on open-source software that anyone can download.

act in the network, only authorized devices can take part as nodes and add blocks. Permissionless and permissioned blockchains also differ for the permission to access the ledger and read transactions. Indeed, permissionless blockchains are usually public, so they have a high degree of openness and anyone can read the transactions. Instead, permissioned blockchains are generally private, because transactions are only visible to authorised users. The reason is that permissionless blockchains are general purpose and do not belong to anyone. In contrast, permissioned blockchains are specifically built to fit a specific purpose of a single entity or a consortium that decided to invest in setting up and maintain the entire system (hardware and software).
As concerns smart contract transactions, firstly a user has to initiate an operation of the smart contract. In doing so, the user has to connect to a node. The algorithm applies to the current state of the smart contract and then computes the next state of the smart contract. When the latter state is determined, a transaction is built. Then, several nodes (validation nodes) have to certify whether the transaction is valid. Each validation node re-executes the operation starting from the original state and checks whether it gets to the same new state. In case of a positive answer, the transaction is valid. If the transaction is valid, all nodes of the network add it to the blockchain. Consequently, all copies of the smart contract in the network change their current state.[23]

3. Smart contracts in the light of contract law

"Smart contract" is a misleading expression. It recalls legal contracts. When Nick Szabo theorised to embed contractual clauses in the hardware and software, «in such a way to make breach of contract expensive», he talked of "smart contracts".[24] With the advent of blockchain technology, this idea has become implementable.[25] Indeed, in the beginning, blockchain technology developed to exchange virtual currencies. Subsequently, it allowed the recording of every digital asset. The most advanced blockchain applications allow the uploading of deterministic computer programs that automatically execute according to predetermined conditions.[26] Therefore, blockchain technology also permits to perform contractual agreements. For this reason, when discussing this blockchain functionality it is usual to refer to it as "smart contract".[27]
Smart contracts are not necessarily contracts. A smart contract *per se* is a computer code that, upon the occurrence of a specific condition, is capable of running auto-

[23] C. Sillaber - B. Waltl, *Life Cycle of Smart Contracts in Blockchain Ecosystems*, in *Datenshutz und Datensichrheit*, 8, 2017, 497.

[24] N. Szabo, *The idea of Smart Contracts,* 1997.

[25] On notion and characteristics of smar contracts, see R. Weber, *Smart Contracts: Do we need new legal rules?*, in A. De Franceschi - R. Schulze - M. Graziadei - O. Pollicino - F. Riente - S. Sica - P. Sirena (eds.), *Digital Revolution – New Challenges for Law. Data Protection, Artificial Intelligence, Smart Products, Blockchain Technology and Virtual Currencies*, München, 2019, 301-303.

[26] Melanie Swan divides blockchain development in Blockchain 1.0, 2.0, and 3.0. See M. Swan, *Blockchain. Blueprint for a new economy,* Sebastopol, 2015.

[27] E. Mik, *Smart contracts,* cit., 273.

matically. This code can be stored and processed on a blockchain and any change is recorded in the blockchain.[28] In theory, smart contracts can automate everything. For example, a smart thermostat that regulates the temperature inside a house according to predetermined settings is a smart contract. In these cases, smart contracts have no legal significance. They acquire legal connotations when they are used to automate legally relevant actions or operations. For instance, a smart contract might issue an administrative authorisation when all the requirements to obtain it are fulfilled.

When smart contracts are used in the contractual domain, someone suggested talking about "smart legal contracts". Usually, researchers distinguish between smart legal contracts as contracts or as means to perform already existing contracts. [29] The latter refers to the use of computer code to automate the performance of an agreement (totally or partially) that formed outside the blockchain, independently of how the agreement was reached.[30] In this hypothesis, the smart contract is not a contract, but it is the tool through which a contract is performed. Automated performance replaces performance of the obliged party. The former hypothesis has regard to the possibility to express an agreement in the form of lines of code. On this point, it is questioned whether smart legal contracts can be contracts.[31] To answer the question, someone rightly starts from the legal definition of contract.[32]

A contract is a legally binding agreement between two or more parties.[33] So, the agreement constitutes the very basis of the contract. The mutual consent of the parties (the agreement) is reached through the exchange of an offer and an acceptance. Another fundamental requirement is the parties' expression of their intention to be legally bound by the contract. This means that the offeror and the offeree intended to enter an agreement apt to produce legal effects within a legal system.

In order to reach the so-called "meeting of the minds", both parties must express their intent in some forms. According to the principle of informality, in the silence of law, the parties are free to choose any form to conclude contracts. [34] This principle allows the conclusion of contracts in electronic form. Another internationally recognised principle supports this statement, which is the principle of non-discrimina-

[28] This definition of smart contract appears in J. Earls *et al.*, *Smart contracts: is the law ready?*, Chamber of Digital Commerce Report, 2018, 10.

[29] E.g. see O. Rikken *et al.*, *Smart contracts as a specific application of blockchain technology,* in *dutchblockchaincoalition.org*, 2017, 22; A. Savelyev, *Contract law 2.0: "smart" contracts as the beginning of the end of classic contract law*, Higher School of Economics Research Paper no. WP BRP 71/LAW/2016, 2016, 9; Smart Contracts Alliance, *Smart contracts: 12 Use Cases for Business & Beyond*, Chamber of Digital Commerce, 2016, 40; G. Finocchiaro, *Il contratto nell'era dell'intelligenza artificiale*, in *Rivista Trimestrale di Diritto e Procedura Civile*, 2, 2018, 443 ss.

[30] E.g. the contract could be concluded through access to a website, by e-mail, orally or in written form at the contemporary presence of two (or more) parties.

[31] E.g. see K. Werbach - N. Cornell, *Contracts Ex Machina*, in *Duke Law Journal*, 67, 2017, 338; J. G. Allen, *Wrapped and Stacked: "Smart Contracts" and the Interaction of Natural and Formal Language*, in *European Review of Contract Law,* 4, 2018, 319.

[32] K. Werbach - N. Cornell, *Contracts Ex Machina*, cit., 338.

[33] See G. Christandl, *Formation of contracts*, in N. Jansen - R. Zimmermann (eds.), *Commentaries on European contract laws*, Oxford, 2018, 236 ss. See also PECL 2:101, DFCR II.-4:101.

[34] PICC 1.2, PECL 2:101(2), DFCR II. – 1:106.

tion.[35] Consequently, contracts can also be expressed in the form of computer code. However, the creation of a smart legal contract does not automatically imply the conclusion of a contract in the lack of a legally binding agreement. Therefore, smart legal contracts can be considered contracts only in the presence of a legally binding agreement. As Sillaber and Waltl observe, «although a smart contract has been stored on the blockchain, this fact alone should not be considered as a party's agreement to enter the contract as anybody can submit any smart contract to the blockchain indicating an obligation for any random wallet owner».[36]

The meeting of the minds (exchange of offer and acceptance) may occur in various ways. Durovic and Janssen stress that smart legal contracts can be concluded either off-chain or on-chain.[37] The authors explain the process of formation of on-chain contracts by referring to the upload of a proposed contract in coding language in the Ethereum platform and its following acceptance by a participant in the Ethereum network that communicates with the uploaded smart contracts (for example by making a payment in ethers). In other terms, a smart legal contract is formed inside the blockchain when a smart contract code is uploaded to the blockchain, but there is not still an agreement on it. Here, the smart contract represents, in combination with the blockchain, the tool through which a user expresses her contractual will.[38] If the will of the user who uploaded the smart contract matches with the one of another user, a contract is formed, and the smart contract becomes a smart legal contract. The formation of smart legal contracts on-chain is more interesting because the blockchain is a new technology. Indeed, smart contracts without the blockchain have been existing for several years.[39]

The following sections put in correlation contract requirements with the formation of blockchain-based smart contracts. The scope of the analysis is to verify how to interpret the rules on contract formation to make blockchain-based smart contracts fit into contract law.

4. Offer and acceptance

The agreement between the parties required to form a valid contract normally con-

[35] Art. 5 of the MLEC and Art. 8(1) of the United Nations Convention on the Use of Electronic Communications in International Contracts. Art. 46 of the Regulation (EU) 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 (e-IDAS Regulation) establishes that «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».

[36] C. Sillaber - B. Waltl, *Life Cycle of Smart Contracts,* cit., 498-499.

[37] M. Durovic - A. Janssen, *The Formation of Blockchain-based Smart Contracts in the Light of Contract Law*, in *European Review of Private Law*, 6, 2019, 760.

[38] *Ibid.*

[39] F. Di Ciommo, *Smart contracts and (non)law. The case of financial markets*, in *Law and Economics Yearly Review*, 7, 2018, 303.

sists of an offer and a corresponding acceptance.[40]

Some authors observe that when a party uploads a smart contract to the blockchain, the uploading[41] corresponds to an offer.[42] The offer must contain all the elements of a valid contract. Otherwise, there is not an offer but an invitation to the other party to enter into negotiations.[43] On this point, Durovic and Janssen consider that «as the "offeror" posts his "contract" onto the blockchain in a binary computer code which specifies precisely the terms of the transaction, it will regularly be held to constitute an offer, not an invitation to treat».[44]

An offer can be directed towards one or more specific persons. Alternatively, it can be addressed to the general audience (proposal to the public).[45] In a blockchain, this depends on the possibility of one or more participants to interact with the smart contract code.[46] More specifically, and from a technical point of view, if the operations of the smart contract are restricted to a specific address (or wallet, or user's profile) in the blockchain, the offer is directed towards a specific participant in the blockchain. In the opposite case, any participant in the blockchain can send transactions, so the offer is open to the general public.

Turning to acceptance, it does not have to meet any specific requirements apart from the offeree's agreement on all the terms of the offer. Therefore, once the offeror has uploaded the smart contract, the offeree could accept it by signing a transaction with a private key.[47]

If the declaration of the offeree does not refer to all the terms of the offer or does not consent to the precise terms of the offer, it is not an acceptance but rather a counter-offer.[48] In the latter case, the counter-offer has to be followed by an acceptance to form a contract. Here, the problem is the immutability of blockchain technology. The code of the smart contract cannot be modified in the blockchain. Consequently, there is no other option than to accept (or to not accept) it.[49] The offeree would need

---

[40] J.M. Smits, *Contract law-a comparative introduction,* Northampton, 2017, 41.

[41] The smart contract code is uploaded on a local node of the blockchain through a "deploy" transaction. Then, the smart contract is replicated in all the nodes of the blockchain.

[42] J. Earls *et al.*, *Smart contracts,* cit., 15; M. Durovic - A. Janssen, *The Formation of Blockchain-based Smart Contracts,* cit., 762.

[43] J.M. Smits, *Contract law-a comparative introduction,* cit., 43 ss. See also Arts. PICC 2.1.2, PECL 2:201, DCFR II. – 4:201 and Art. 11 of the UN Convention on the Use of Electronic Communications in International Contracts.

[44] M. Durovic - A. Janssen, *The Formation of Blockchain-based Smart Contracts,* cit., 762.

[45] J.M. Smits, *Contract law-a comparative introduction,* cit., 44 ss. See also Arts. PECL 2:201 (2) and DFCR II. – 4:201 (2).

[46] J. Earls *et al.*, *Smart contracts,* cit., 17; J. Madir, *Smart Contracts: (How) Do They Fit Under Existing Legal Frameworks?*, in *Social Science Research Network (SSRN)*, 14 December 2018, 7.

[47] J. Earls *et al.*, *Smart contracts,* cit., 17; J. Madir, *Smart Contracts*, cit., 7.

[48] J.M. Smits, *Contract law-a comparative introduction,* cit., 54.

[49] Carron and Botteron talk about a "take it or leave it" offer. See B. Carron - V. Botteron, *How smart can a contract be*, in D. Kraus - T. Obrist - O. Hari (eds.), *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law*, Northampton, 2019, 124; Werbach and Cornell argue that smart contracts are by default unilateral because only one party places them on the blockchain. See K. Werbach - N. Cornell, *Contracts Ex Machina*, cit., 343.

to upload a new smart contract and upload it to the blockchain. The upload would correspond to a new offer and the offeree would become the offeror.
The acceptance can occur also in the absence of a specific declaration when it is implied by the offeree's conduct.[50] More precisely, if the offeree starts performing the contract, her actions can be considered as a valid acceptance of the offer. Un unequivocal behavior of the offeree showing a clear acceptance is required. In a blockchain, for example, ceding control over a certain amount of money to the code can be considered acceptance.[51]

5. Time of conclusion of the contract

Establishing the exact time of contract conclusion is of huge importance. From that moment, indeed, the parties are legally bound by the contract, and the contract is in abstract apt to produce its legal effects. In addition, at the time a contract is concluded the offeror can no longer revoke her offer.[52] The time of conclusion of a contract can be determined easily if the parties are present or make use of an instantaneous means of communication. It is more problematic when the parties are absent and a certain amount of time passes between offer and acceptance.[53] If that is the case, the time of conclusion of a contract varies according to the applicable legal system. In general, there are three main rules: 1) the dispatch rule (known also as 'mailbox' or 'postal' rule), where acceptance becomes effective at the moment of sending; 2) the receipt rule, which determines that a contract is considered concluded when the offeror receives the acceptance; 3) the actual notice rule, according to which a contract is formed when the offeror acquires knowledge of the acceptance.[54] Anyway, the jurisdictions that adopt the actual notice rule mitigate it by presuming that the offeror acquires knowledge of the acceptance when it reaches her address unless the offeror proves that acquiring knowledge of the acceptance was impossible for reasons not dependent on her fault.[55]
In the field of electronic contracts, these rules apply by bearing in mind the principle of functional equivalence.[56] Proposal and acceptance are sent or received in the form

[50] J.M. Smits, *Contract law-a comparative introduction,* cit., 57-58. See Arts. PICC 2.1.6 (3), PECL 2:204 (1) and DFCR II. – 4:204(1).

[51] M. Raskin, *The Law and Legality of Smart Contracts*, in *Georgetown Law Technology Review*, 1, 2017, 322; B. Carron - V. Botteron, *How smart can a contract be,* cit., 128 take the example of the transfer of cryptocurrencies by an investor in an ICO. M. Durovic - A. Janssen, *The Formation of Blockchain-based Smart Contracts,* cit., 762-763 imagine the uploading of a smart contract for the transferring of the ownership of a car for 10 ethers, and state that the upload of the 10 ethers by an offeree is an acceptance done by conduct.

[52] G. Christandl, *Formation of contracts,* cit., 323.

[53] Ivi, 324 ss.

[54] The dispatch rule is typical of Common Law. The receipt rule applies to Austria, Germany, and France. Moreover, it is followed by the PICC, the PECL, and the DFCR. The actual notice rule is applied in Italy and Spain.

[55] Art. 1326 (1) *Codice Civile* and Art. 1262 (2) *Código civil.*

[56] The MLEC and the United Nations Convention on the Use of Electronic Communications in

of data messages by means of electronic addresses. The dispatch rule implies that a contract is concluded when the electronic communication that represents the acceptance leaves the information system under the control of the offeree,[57] while, following the receipt rule, the time of conclusion is when the electronic message that contains the acceptance reaches the offeror's information system and can be accessed by the offeror.[58] The latter is also valid with the actual notice rule unless the offeror demonstrates that she was unable (without fault) to know about the acceptance.[59]

In a white paper by R3 and Norton Rose Fulbright,[60] the conclusion of a smart legal contract on the blockchain is compared to the exchange of data messages through e-mails because in the blockchain offer and acceptance are expressed by data messages sent using public-key infrastructure through an Internet connection. Indeed, according to the MLEC and the UN Convention on the Use of Electronic Communications in International Contracts, a data message is any information generated, sent, received or stored by electronic, magnetic, optical or "similar means".[61] This definition

International Contracts established the principle of functional equivalence. The principle is based on an analysis of the purposes and functions of the traditional paper-based requirement to determine how those purposes or functions could be fulfilled through electronic-commerce techniques. H.D. Gabriel, *The United Nations Convention on the Use of Electronic Communications in International Contracts: an Overview and Analysis*, in *Uniform Law Review*, 11, 2006, 285. M. Ratti, *La Convenzione sull'uso delle comunicazioni elettroniche: le principali disposizioni,* in G. Finocchiaro - F. Delfini (eds.), *Diritto dell'informatica*, Milano, 2014, 71. About the use of metaphors to describe the world of the web in the transition from the the real space to the cyberspace, see A. Morelli - O. Pollicino, *Le metafore della rete. Linguaggio figurato, judicial frame e tutela dei diritti fondamentali nel cyberspazio: modelli a confronto*, in *Rivista AIC*, 1, 2018, 1.

[57] Art. 15 of the MLEC establishes the time of dispatch of a data message. Art. 10(2) of the UN Convention on Electronic Communications defines the time of dispatch of electronic communication. See W. Kilian, *Time and Place of Dispatch and Receipt*, in A. H. Boss - W. Kilian (eds), *The United Nations Convention on the Use of Electronic Communications in International Contracts: An In-depth Guide and Sourcebook*, Austin - Boston - Chicago - New York - the Netherlands, 2008, 162.

[58] DFCR I. – 1:109 (4)(c) provides that a notice transmitted by electronic means reaches the address when it can be accessed by the addressee. According to Art. 10(2) of the United Nations Convention on the Use of Electronic Communications in International Contracts, electronic communication is presumed to be capable of being retrieved by the addressee when it reaches the addressee's electronic address. See also Art. 15(2) of the MLEC. I. Schwenzer - F. Mohs, *Old Habits Die Hard: Traditional Contract Formation in a Modern World*, in *Internationales Handelsrecht*, 6, 2006, 236.

[59] As reported by M. Giancaspro, *Is a "smart contract" really a smart idea? Insights from a legal perspective*, in *Computer Law & Security Review*, 33, 2017, 825, in England, when an offer is accepted via technology, acceptance becomes effective upon receipt, as opposed to the dispatch rule for traditional contracts (regulation 11 of the Electronic Commerce Regulations 2002). The reason is that the dispatch rule was conceived as a compromise between the free revocability of the offer until conclusion and the need to protect the offeree. Indeed, with traditional ways of communication for concluding contracts at a distance, acceptance could have taken a lot of time before arriving at destination. So, the offeree should have been able to accept a contract with the certainty that it would have been binding. Now, because offer and acceptance are exchanged instantaneously, the dispatch rule has lost its function. See A. Rawls, *Contract Formation in an Internet Age*, in *Columbia Science and Technology Law Review*, X, 2009, 207 ss; E. Mik, *The Effectiveness of Acceptances Communicated by Electronic Means, or – Does the Postal Acceptance Rule Apply to Email?*, in *Journal of Contract Law*, 26, 2009, 8. The same is in Australia, while in the USA the dispatch rule applies even when acceptance occurs via the Internet. In France, French courts usually decide on a case-by-case basis.

[60] R3, Norton Rose Fulbright, Can smart contracts be legally binding contracts?, R3 and Norton Rose Fulbright White Paper, November 2016, 22.

[61] Art. 2(1)(a) of the MLEC and Art. 4(1)(c) of the United Nations Convention on the Use of Electronic Communications in International Contracts.

was intended to apply to all existing communication techniques and all types of paperless messages.[62] Moreover, as with e-mails, the offeror and the offeree do not make use of an instantaneous means of communication (such as the telephone) but they are absent and a certain time passes between offer and acceptance.

These data messages are sent and received using electronic addresses, i.e. the accounts that every user has to create to take part in the blockchain and to send transactions.[63] There is no difference with electronic commerce, where the offer and the acceptance are sent from an electronic address or received by an electronic address in the form of data messages. For this reason, the dispatch, the receipt, and the actual notice rules have to be interpreted in the same way. Namely, according to the dispatch rule, the contract is concluded when the offeree sends the acceptance (in the form of a data message) by her electronic address; according to the receipt rule, the contract is concluded when the offeror's electronic address receives the acceptance (in the form of a data message); according to the actual notice rule, similarly to the receipt rule, the contract is concluded when the offeror's electronic address receives the acceptance unless the offeror proves that she could not access her information system for reasons not dependent on her fault.

The remaining issue is to establish which acts correspond to the sending and the receipt of the acceptance in the blockchain.[64] In our opinion, the offeree sends her acceptance when she sends the transaction of acceptance from her address to the address of the smart contract after having signed it with her private key. As concerns the receipt, we think that the offeror receives the acceptance when the transaction of acceptance also reaches her node after having been validated. Indeed, valid transactions are replicated in all nodes of the blockchain network.

In summary, according to the dispatch rule, the contract is concluded when the offeree sends the transaction of acceptance after having signed it with her private key; according to the receipt and the actual notice rule, the contract is concluded when the transaction of acceptance reaches the offeror's node (under the actual notice rule, the offeror can prove that he could not acquire knowledge of it for reasons not dependent on her fault). The application of the dispatch rule, the receipt rule, or the actual notice rule depends on the applicable law.

In case of acceptance by conduct, the contract is concluded through the performance of the contract by the offeree.[65] This statement does not need further interpretations in the domain of blockchain-based smart legal contracts.

---

[62] A. Mukherjiee, *Smart Contracts – Another Feather in UNCITRAL's Cap*, in *Cornell International Law Journal Online*, 8 February 2018.

[63] See section 2.

[64] According to M. Giancaspro, *Is a "smart contract" really a smart idea?,* cit., 830 «The obvious question is whether acceptance occurs once the party seeking to purchase the goods transmits their offer, once it is received and authenticated through consensus of network users, or once it is coded and added to the blockchain».

[65] PICC 2.1.6(3), PECL 2.205 (3), DFCR II. – 4:205 (3).

6. Contractual intention

As mentioned above, in addition to the meeting of the minds, parties must have the intention to be legally bound to their agreement. When a contract is expressed with the language of the code, because the average man is not capable to understand it, it is questioned whether it can be said that the accepting party had the intention to conclude a contract and to be bound by it.[66]

According to the prevailing view, contractual intention has to be objective and not subjective, in the sense that it does not matter the inner intention of the party, her perceptions or understanding. To protect the expectations of the other party and to preserve efficiency and legal certainty of contractual relationships, the agreement must be understood from the external perspective of a reasonable observer. An objective evaluation of the party's statements or conduct has to be carried out by taking into account the circumstances of the case and the general principle of good faith.[67]

In the light of that, the law pays much attention to contractual intention when terms are drafted unilaterally and not individually negotiated between the parties, as is for contracts with standard terms and conditions. It is wondered whether the non-drafting party can be considered bound by the contract. It is today generally acknowledged that the drafting party has to take reasonable steps to bring terms to the other party's attention when the contract is made or beforehand.[68] «To take reasonable steps» means that «[…]the supplier has to take care that the other party is actually aware of those terms and may easily read them».[69] Similarly, Annex I(1)(i) of the Unfair Contract Terms Directive[70] states that the consumer should have a «[…]real opportunity of becoming acquainted» with the terms «[…]before the conclusion of the contract», otherwise the term is considered unfair and does not bind the consumer. The Directive only refers to B2C contracts. Indeed, consumers are the weakest party and need a higher level of legal protection.

The existence of contractual intention has also been discussed about "wrap contracts", which are adhesion contracts concluded online. The most common wrap contracts are "click-wrap" and "browse-wrap" agreements. They are presented and concluded in a non-traditional manner. Indeed, in a click-wrap agreement, the terms are presented in a scrollable box or at a hyperlink, and the other party has to click on an "I agree" button to accept. In a browse-wrap agreement, the terms are accessible through hyperlinks ("Terms of use" or "Legal terms") and the user accepts using a website or downloading the digital content, without having to click on the "I agree" box or take any other positive action. In both cases, courts have expressed the need to provide

[66] B. Carron - V. Botteron, *How smart can a contract be,* cit., 128 ss; Pinsent Masons, Smart insurance Contracts: A discussion paper by Pinsent Masons and Applied Blockchain, 2017, 12; R. O' Shields, *Smart Contracts: Legal Agreements for the Blockchain*, in *North Carolina Banking Institute*, 21, 2017, 186.

[67] J.M. Smits, *Contract law-a comparative introduction,* cit., 64-70. See also PECL 2:102 and DFCR II.-4:102.

[68] See N. Jansen, *Art. 2:104: Terms not Individually Negotiated*, in N. Jansen - R. Zimmermann, *Commentaries on European contract laws*, cit., 272 ss. See PICC 2.1.19, PECL 2:104, DFCR II.-9:103.

[69] Ivi, 278.

[70] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.

the other party with sufficient notice of the existence of the terms before or at the time of contract conclusion.[71] In this regard, it is not sufficient to give notice of the existence of the terms, but the terms have to be conspicuously and clearly presented to the non-drafting party. Therefore, the supplier has to take care that the other party is (or should be reasonably) aware of being entering into a contract. Without these arrangements, it has been argued that in browse-wrap contracts it is unlikely that the non-drafting party is aware of the existence of a contract because she is not required to take any positive assenting action. Similarly, in click-wrap contracts, online users do not give importance to the action of clicking on a box as they do with the physical act of placing a signature. In the latter case, however, a higher level of awareness is presumed because the offeree is asked to do something to enter the agreement.

To summarise, in adhesion contracts – being them in paper or online – it is necessary to provide the other party with the terms of the contract in a clear and comprehensible version for the average man in ways that allow her to become reasonably aware of being entering a contract. Otherwise, it cannot be affirmed that the non-drafting party intended to conclude a contract.

Taking account of the above, we think that the fact alone that the contract is expressed in computer code does not suffice to exclude contractual intention. The accepting party has the duty to get informed and understand what she is doing before accepting the offer. Instead, it should be considered the circumstances that preceded the conclusion of the contract, and the qualities of the accepting party.

It has been already described[72] that in on-chain contracts there are "take it or leave it" offers, in the sense that because of the immutability of the blockchain there is not the possibility to make a counter-offer. The contract is drafted unilaterally, and the other party has no other option to accept or not accept it, as is with adhesion contracts. We also find similarities with wrap contracts because of the non-traditional way of expressing assent. Indeed, once the offeror has uploaded the smart contract code on the blockchain, the offeree can accept it by sending some data to the address of the smart contract (e.g. by signing a transaction of acceptance with a private key or by transferring a certain amount of cryptocurrencies). In this event, only one party drafts the terms of the contract, using a non-comprehensible language (at least for the average man), and those terms are accepted in a non-traditional way. For these reasons, we believe that the offeror should accompany the code with a natural language version of the terms, in a clear and comprehensible manner. Moreover, the other party should have the opportunity to understand the moment in which she is going to enter into a contract. For example, O'Shields talks of the possibility to provide an "I agree" button;[73] McKinney, Landy and Wilka propose a check-box or "execute" button.[74]

---

[71] On this topic, see R. Momberg, *Standard terms and transparency in online contracts*, in A. De Franceschi (ed.), *European Contract Law and the Digital Single Market – The Implications of the Digital Revolution,* Cambridge –Antwerp – Portland, 2016, 189 ss.

[72] Section 4.

[73] R. O' Shields, *Smart Contracts,* cit.,186.

[74] S. A. McKinney - R. Landy - R. Wilka, *Smart contracts, blockchain, and the next frontier of transnational law*, in *Washington Journal of Law, Technology & Arts*, 13, 2018, 326.

The distinction between B2B and B2C contracts is also relevant. Businesses usually have more bargaining power than consumers. For example, they may have greater economic possibilities to consult an expert that can understand the language of the code. It might also happen that the contract is concluded based on a pre-existing framework agreement that set the main object of future contracts and the modalities of their conclusion on-chain.[75]

7. The e-Commerce Directive and the Consumer Rights Directive. Information requirements

The Directive 2000/31/CE on electronic commerce and the Directive 2011/83/EU on consumer rights in distance and off-premises contracts include some rules that apply before or at the moment of placing an online order. So, it is important to verify whether these rules are also applicable to the formation of blockchain-based smart legal contracts.

The e-Commerce Directive approximates certain national provisions on information society services also relating to electronic contracts,[76] i.e. contracts concluded at a distance and by electronic means.[77] "Electronic means" refer to «[…]electronic equipment for processing (…) and storage of data».[78] We think that there are no obstacles to the application of the Directive. The offeror and the offeree do not make use of an instantaneous means of communication but they are absent and a certain time passes between offer and acceptance. Moreover, the offeror instantiates a smart contract and the offeree accepts the contract by sending a data message to the smart contract code. Both use a public-key infrastructure and an Internet connection. A distributed and decentralised electronic ledger (the blockchain) processes and stores the offeror's uploading, the offeree's data message, and the resulting change of state of the smart contract code.

Similarly, the Consumer Rights Directive apply to distance contracts, that is «any contract concluded between the trader and the consumer under an organised distance sales or service provision scheme without the simultaneous physical presence of the trader and the consumer, with the exclusive use of one or more means of distance communication up to and including the time at which the contract is concluded».[79] Recital 20 also considers mail orders and the Internet as means of distance communication. Other provisions explicitly refer to distance contracts concluded by electronic

[75] Especially if the parties transact through a permissioned blockchain set up for specific purposes.

[76] See Art. 1(2) of the Directive.

[77] According to Art. 2(1)(a) of the Directive, «information society services[…]» are «[…]services within the meaning of Art. 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC», i.e. any services normally provided for remuneration, at a distance and by electronic means at the individual request of a recipient of services.

[78] See recital 17 of the Directive.

[79] See Art. 2(7) of the Consumer Rights Directive.

means.[80] So, we believe that the Directive is also applicable to contracts concluded on-chain for the same reasons expressed for the e-Commerce Directive about the at a distance and electronic nature of such contracts (even though the Directive 2011/83/EU only concerns B2C contracts).

That clarified, both Directives set down some information requirements that the service provider or the trader shall provide to the recipient of the service or the consumer.[81] Art. 10 of the e-Commerce Directive establishes that such information requirements are not mandatory in B2B contracts, while those laid down in the Consumer Rights Directive only refer to B2C contracts.[82] Art. 10 of the e-Commerce Directive also states that the provision shall not apply to contracts concluded exclusively by exchange of electronic mail or by equivalent individual communications.

It could be questioned whether the on-chain modality of conclusion of smart legal contracts can be considered an equivalent individual communication like electronic mail.

In that regard, we already explained that in blockchain the offeror can direct her offer towards one (or more) specific person(s) or to the public. In the former hypothesis, only authorised blockchain addresses can interact with the smart contract code, while in the latter any participant in the blockchain can send data messages to the smart contract code. When the offeror directs the offer towards one (or more) specific person(s) we think that the contract is concluded by a form of individual communication equivalent to electronic mail. Indeed, the fact that the offeror indicates one (or more) specific address(es) means that she has already identified the recipient(s) of the offer. In the opposite case, the recipient of the offer is indifferent to the offeror, as is when a business makes available her offer on a website. So, we assume that when the offeror addresses her offer to one (or more) determined recipient(s), the information requirements laid down in Art. 10 of the e-Commerce Directive do not apply.

Maybe, this form of individual communication is more frequent in permissioned blockchains[83] because they are closed systems with known participants.

Another question is whether these information requirements can be expressed in the language of the code. On this point, we think that there are two main obstacles, one technical and one legal.

About the former, someone has observed that not all contractual conditions are operational. There are non-operational contractual conditions, such as those that determine the applicable law or jurisdiction.[84] Similarly, information requirements need a descrip-

[80] See Art. 8(2) and Art. 11(3).

[81] Art. 5 and 10 of the e-Commerce Directive; Art. 6 of the Consumer Rights Directive.

[82] Art. 6(8) of the Consumer Rights Directive states that these information requirements are in addition to information requirements contained in the e-Commerce Directive.

[83] Section 2.

[84] E. Mik, *Smart contracts: terminology, technical limitations and real world complexity,* cit., 294. In general, there are huge difficulties to embed a contract in the form of computer code. Computer language is not flexible, while flexibility allows the adaptation of the contract to all future circumstances and to the context; it does not consider that contracts are by their nature incomplete and have to be supplemented through gap-filling. About this, see J. G. Allen, *Wrapped and Stacked,* cit.; J. M. Sklaroff, *Smart contracts and the cost of inflexibility*, in *University of Pennsylvania Law Review*, 166, 2017, 263; P. Cuccuru, *Beyond Bitcoin: an*

tive, and non-operational, language.

From a legal point of view, both Directives stress the importance of transparency of information. Art. 5(2) of the e-Commerce Directive states that «where information society services refer to prices, these are to be indicated clearly and unambiguously»; Art. 10 of the same Directive dictates that the information is given by the service provider «clearly, comprehensibly and unambiguously». Art. 6 of the Consumer Rights Directive establishes that the provider shall provide the consumer with the information «in a clear and comprehensible manner».

With the advent of the Internet and the development of electronic commerce, people started to conduct their affairs without knowing the identity of the counterparty and without the possibility to directly test the quality of desired services and products. Indeed, the Internet is an open network that permits communication between strangers. They conclude contracts by navigating on websites made available by businesses or intermediary platforms that display virtual icons and buttons that may disorient customers.[85] This led to a lack of trust in the online market. For this reason, traditional contract law needed to be accompanied by further norms to encourage electronic contracting. [86] Among them, information requirements help the other party to become aware of the conclusion of the contract and its contents. In other words, they aim to enhance trust in electronic and distance contracts. A higher level of protection is needed in B2C contracts, where the consumer is the weakest party, and in contracts concluded by access to a website because the identity of the other party is unknown and the terms of the contract are arranged unilaterally. For these reasons, according to the e-Commerce Directive, information requirements are mandatory in B2C contracts and applicable to all contracts not concluded with electronic mail or other equivalent individual forms of communication. The latter modality of contract conclusion is more suitable for parties that already know each other and that are both involved in the process of the drafting of the contract.

In the previous section, we assumed that smart legal contracts should be provided in natural language when the parties have a different bargaining power (such as in B2C contracts), the contract is drafted unilaterally and the accepting party has not the capacity to understand the language of the code. In this way, the party can become reasonably aware of the contract. Therefore, we believe that also information requirements should be given in natural language (in a clear, unambiguous and comprehensible manner) in the same cases where they are mandatory, i.e. in B2C contracts and when the on-chain modality of conclusion of smart legal contracts cannot be considered an equivalent individual communication.

early overview on smart contracts, in *International Journal of Law and Information Technology*, 25, 2017, 179.

[85] The so-called "wrap agreements". See the previous section.

[86] G. Pearce - N. Platten, *Promoting the Information Society: The EU Directive on Electronic Commerce*, in *European Law Journal*, 6, 2000, 363; G. Finocchiaro, *Il perfezionamento del contratto on line: opportunità e criticità*, in *Diritto comunitario e degli scambi internazionali*, 1-2, 2018, 187. About the impact of the Internet on law, see O. Pollicino - M. Bassini, *Internet Law in the Era of Transnational Law*, EUI Working Paper RSCAS 2011/24; O. Pollicino - M. Bassini, *The Law of the Internet between Globalization and Localization*, in M. Maduro - K. Tuori - S. Sankari (edss), *Transnational Law – Rethinking European Law and Legal Thinking*, Cambridge, 2014, 346 ss.

Lastly, because information requirements have the purpose of strengthening the offeree's confidence in the other party's, De Graaf[87] reflects on the practical need of information requirements for blockchain-based smart legal contracts. He argues that «Many commercial parties that wish to sell products or services on the Internet gave an interest in complying with those laws. Traditionally, they sell more when buyers trust them. And one way to gain trust is by providing information about yourself and by complying with internet laws. However, there is no (or less of a) need to do so with smart contracts. Because smart contracts execute themselves, trust in the code is important, not trust in the supplier».[88] In the opinion of the author, the obliged party cannot control the computer system that performs the contract on her behalf thanks to the immutable character of blockchain. By uploading the smart contract to the blockchain, the party cannot refuse to perform. There is no more need to trust in the other party – that cannot avoid execution – but in the code.

Taking apart any considerations regarding the actual capacity of blockchain technology to avoid the control of the obliged party on the performance of the contract, which should be dealt with separately, information requirements do not only contribute to the identification of the party. De Graaf rightly observes that «If the supplier feels no need to comply with these laws and (therefore) also does not provide information about himself, enforcements by courts of law becomes difficult, if not impossible. And if the supplier has no physical address and his assets are unknown, it is difficult to litigate against him and execute his assets if he is ordered by a court to pay a sum of money».[89] Information requirements do not only concern the identity of the obliged party or her geographical address of establishment – which allow the enforcement of the contract - but also the products and services offered, the prices, the technical steps to follow to conclude the contract, the places and the modalities of access to the terms of the contract, the technical means for identifying and correcting input errors prior to the placing of the order, the languages of the contract, and so on. In short, information requirements try to empower the awareness of the weaker party's actions so that to rebalance the parties' negotiating position and foster e-commerce. Therefore, even though on the one hand parties might be more confident that the contract is performed thanks to the blockchain, on the other hand, the blockchain does not remove the risk of unaware and disadvantaged parties.

7.1. The acknowledgment of receipt

Art. 11 of the e-Commerce Directive states that in case the recipient of the service places his order, the service provider has to acknowledge the receipt of the recipient's order without undue delay and by electronic means.[90] This duty does not introduce a

[87] T. J. De Graaf, *From old to new: from internet to smart contracts and from people to smart contracts*, in *Computer Law & Security Review*, 35, 2019, 9.

[88] *Ibid.*

[89] Ivi, 9-10.

[90] A similar provision is laid down in DFCR II. – 3:202.

new way for the exchange of offer and acceptance but is intended to give certainty about the conclusion of the contract because the recipient is distant and cannot know if the order arrived at its destination.[91] The acknowledgment of receipt is not mandatory in B2B contracts[92] and shall not apply to contracts concluded exclusively by exchange of electronic mail or by equivalent individual communication.[93] The reasons for these derogations are the same as those concerning information requirements. In short, in these situations, the conclusion of the contract is less risky for the recipient, and the latter can understand more easily whether and when a contract was concluded. Therefore, Art. 11 of the e-Commerce Directive is applicable and not applicable in the same cases information requirements apply or do not apply.[94]
Maybe, the distributed character of blockchain might help to fulfil the function of the acknowledgment of receipt, i.e. to detect the receipt of the order. Indeed, after the validation nodes have validated the transaction of acceptance, the latter is replicated in the nodes of the network and becomes visible.[95] Thus, the blockchain might be useful to give evidence of the receipt of the order.

8. Form

In section 3, we claimed that a contract can also be expressed in the language of the code, according to the principle of informality and the principle of non-discrimination. Smart contracts fall under the definition of electronic document laid down in the e-IDAS Regulation according to which an electronic document is «any content stored in electronic form, in particular text or sound, visual or audiovisual recording».[96] Indeed, smart contracts are computer programs stored on a decentralised ledger.[97] In its report "Blockchain and digital identity" the European Union Blockchain Observatory and Forum affirms that «as fully digital ledgers, blockchains are by definition electronic documents under eIDAS. That means, among other things, that blockchains, or more properly the data, included smart contracts, contained therein, cannot be denied legal force solely because of their electronic nature».[98]

[91] J. K. Winn - J. Haubold, *Electronic Promises: Contract Law Reform and E-Commerce in a Comparative Perspective*, in *European Law Review*, 27, 2002, 575; D. Memmo, *Il consenso nei contratti telematici*, in G. Finocchiaro - F. Delfini, *Diritto dell'informatica,* cit., 503.

[92] Art 11(1).

[93] Art. 11(3).

[94] See the previous section.

[95] This depends on the right to read transactions. As seen in section 2, in permissionless blockchains everyone can read transactions, while in permissioned blockchains this is possible only for authorised addresses.

[96] Art. 3(35).

[97] In the USA, some countries (Arizona, California, Nevada, Tennessee, Ohio) have introduced *ad hoc* rules that recognise all records in the blockchains as electronic records under the Uniform Electronic Transaction Act (UETA). See 2017 Ariz. HB 2417; 2018 Cal. AB 2658; Nev. Rev. Stat. Ann. § 719.090; 2018 Ohio. SB 220 1306.01; 2018 Tenn. SB 1662 47-10-202. See A. J. Bosco, *Blockchain and the Uniform Electronic Transactions Act*, in *The Business Lawyer*, 74, 2018/2019, 243.

[98] See page 21. The report was published on 2 May 2019 and is accessible at *eublockchainforum.eu*.

Sometimes the law requires some formalities for the validity of contracts or to prove their existence.[99] In this regard, the UNCITRAL has adopted the functional equivalence approach.[100]

When the law requires some formalities for the validity or to make evidence of a contract, the parties have usually to sign the contract. [101] When the contract is in an electronic form, it can be signed with electronic signatures. Art. 2(a) of the UNCITRAL Model Law on Electronic Signatures defines electronic signatures as «data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message». According to Art. 3(10) of the e-IDAS Regulation electronic signatures are «data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign». Electronic signatures differ from traditional signatures because the latter are the result of a human gesture, so they are based on graphics. Electronic signatures are the result of a technological procedure and are based on a technique.[102] Hence, it was wondered when electronic signatures could be considered equivalent to handwritten signatures.

On this point, Art. 7(1) of the UNCITRAL Model Law on Electronic Commerce provides that «Where the law requires a signature of a person, that requirement is met in relation to a data message if: (a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and (b) that method is reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all circumstances, including any relevant agreement». The UNCITRAL Model Law on Electronic Signatures and the United Nations Convention on the Use of Electronic Communications in International Contracts contain similar provisions.[103]

These international instruments of hard and soft law have guided countries' legislators. Indeed, many countries have adopted the principle of functional equivalence by setting functional requirements for an electronic signature. In particular, some legislations establish that the courts evaluate the meeting of such requirements on a case-by-case basis, while other legislations have adopted a two-tier approach: those electronic signatures which are based on some form of third party identity certification are con-

[99] J.M. Smits, *Contract law-a comparative introduction,* cit., 101 ss. Formalities have the function to warn a party that she is entering a particularly important or financially dangerous contract (warning function) or to inform the party before she is bound (information function). Formalities to prove the existence of the contract have the function to provide certainty about the existence and the content of contracts (evidentiary function).

[100] See section 5, note No. 55.

[101] Some contracts need to be laid down in a notarial deed in the civil law. In these cases, the parties sign the deed and the notary must establish that the parties intend to be bound after having warned them about the legal consequences of their actions.

[102] G. Finocchiaro, *Article 3. Definitions*, in A. Zaccaria - M. Schmidt Kessel - R. Schulze - A.M. Gambino (eds.), EU *eIDAS Regulation – Article-by-Article Commentary,* München, 2020, 55. See also G. Finocchiaro, *Firme elettroniche e firma digitale*, in G. Finocchiaro - F. Delfini, *Diritto dell'informatica,* cit., 309 ss.

[103] Art. 6 of the Model Law on Electronic Signatures and Art. 9 of the UN Convention on the Use of Electronic Communications in International Contracts.

sidered equivalent to handwritten signatures; for the other electronic signatures, the courts have to evaluate such equivalence.[104]

The e-IDAS Regulation adopts a two-tier approach. It recognises three kinds of signature: the simple electronic signature,[105] the advanced electronic signature,[106] and the qualified electronic signature.[107] Only the latter signature shall have the equivalent effect of a handwritten signature,[108] while for the other evaluations are left to the courts.

In the blockchain, users sign transactions with their private keys. Transactions are data messages exchanged between accounts. As seen in section 4, the first transaction concerning a smart contract is the uploading of a new smart contract code on the blockchain. A user signs a "deploy" transaction. The smart contract code is added to the blockchain and associated with an address. Then, the smart contract code changes its state according to the transactions it receives.

When parties make use of blockchain-based smart contracts for the conclusion of legally binding contracts, the offer is made by uploading the smart contract on the blockchain, and the acceptance occurs by sending a transaction to the address of the smart contract. Both the offeror and the offeree link some data (the private key) to other data (the transactions) and approve the information included in the latter data (offer and acceptance). So, these signatures can be considered at least simple electronic signatures.

Qualified electronic signatures have to be created by a qualified electronic signature creation device and have to be based on a qualified certificate for electronic signatures.[109] A qualified signature creation device is configured software or hardware used to create an electronic signature[110] that meets the requirements laid down in Annex II of the Regulation.[111] The definition of electronic signature creation data is more abstract than the former definition of Directive 1999/93/EC[112] that referred to codes or private cryptographic keys.[113] This is due to the principle of technology neutrality, so the Regulation implicitly also mentions cryptographic private keys when it refers to electronic signature creation data.[114] Cryptographic private keys are also used to sign blockchain transactions.

The requirements of Annex II essentially concern the confidentiality and security of the data for the creation of the electronic signature.[115] According to Art. 29(2) of

104 C. Reed, *Electronic commerce*, in C. Reed (ed), *Computer Law*, Oxford, 2011, 282.

105 Art. 3(10) of the e-IDAS Regulation.

106 Art. 3(11) of the e-IDAS Regulation.

107 Art. 3(12) of the e-IDAS Regulation.

108 Art. 25(2) of the e-IDAS Regulation.

109 Art. 3(12) of the e-IDAS Regulation.

110 Art. 3(22) of the e-IDAS Regulation.

111 Art. 29(1) of the e-IDAS Regulation.

112 The e-IDAS Regulation has repealed the above Directive.

113 Art. 2(4) of the Directive 1999/93/EC.

114 K. Erler, *Article 29. Requirements for Qualified Electronic Signatures Creation Devices*, in A. Zaccaria - M. Schmidt Kessel - R. Schulze - A.M. Gambino (eds.), EU *eIDAS Regulation,* cit., 246.

115 M.C. Meneghetti, *Articolo 3*, in F. Delfini - G. Finocchiaro (eds.), *Identificazione elettronica e servizi*

the Regulation, the Commission can establish reference numbers of standards for qualified electronic signature creation devices. If the device meets those standards, compliance with the requirements of Annex II is presumed. The Commission has not established reference numbers of standards under Art. 29(2). However, it has adopted Implementing Decision (EU) 2016/650[116] under Art. 30(3). Indeed, Art. 30 of the Regulation provides that the conformity of the devices with the requirements of Annex II shall be certified by appropriate public or private bodies that have to carry out a security evaluation process in accordance with standards established by the Commission. So, the standards of Implementing Decision (EU) 2016/650 may give indications for interpreting the requirements of Annex II.[117]

A qualified certificate for electronic signature is a certificate, i.e. an attestation that links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person.[118] It is issued by a qualified trust service provider and shall meet the requirements laid down in Annex I of the Regulation.[119] The certificate has the function to link the signature to an identified subject. If the certificate is qualified, there is a higher level of security in the connection between a signatory and a signature.[120] A qualified trust service provider is a natural or legal person that provides qualified trust services and is granted the qualified status by the supervisory body.[121]

Despite the principle of technology neutrality and the elaboration of a list of generic requirements, an essential element of a certificate is a particular system of electronic signature, i.e. the PKI Infrastructure,[122] which is also used to validate signatures in the blockchain. Indeed, we described in section 2 that blockchain makes use of asymmetric cryptography. Each user is provided with a pair of keys, one public and one private. The private key is secret and is used to sign transactions. The public key is known by anyone.

In light of the above, despite transactions in the blockchain are signed through cryptographic private keys, and a PKI infrastructure is used, electronic signatures can be considered qualified only in the presence of a qualified signature creation device and a qualified certificate. Therefore, the wallet that contains the keys should meet some

fiduciari per le transazioni elettroniche nel mercato interno, commento al regolamento UE 910/2014, Torino, 2017, 43.

[116] Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Arts. 30(3) and 39(2) of Regulation (EU) No 914/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market [2016] OJ L 109/40.

[117] K. Erler, *Article 29,* cit., 251. Art. 1(1) of the Decision specifies that the standards apply where the electronic signature creation data is held in an entirely but non-necessarily exclusively user-managed environment. Otherwise, in the case a qualified trust service provider manages the device, the certification shall be based on a process that, pursuant to Art. 30(3)(b) of the Regulation, uses comparable security levels (Art. 1(2)). Art. 30(3)(b) of the Regulation provides that such comparable security levels shall apply in the absence of standards.

[118] Art. 3(14) of the e-IDAS Regulation.

[119] Art. 3(15) of the e-IDAS Regulation.

[120] M. C. Meneghetti, *Articolo 3,* cit., 44.

[121] Art. 3(20) of the e-IDAS Regulation.

[122] Public-Key Infrastructure. See G. Finocchiaro, *Article 3. Definitions*, cit., 58-59.

requirements that guarantee confidentiality and security of the electronic signature creation data, and there should be a certificate issued by a qualified trust service provider that attests the link between the keys and a precise identity.[123]

An electronic signature can be considered advanced if it meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; (d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.[124]

We think that the use of PKI in the blockchain satisfies requirement (a). Asymmetric cryptography – i.e. the private and the public key that every user holds to transact - is resistant to unauthorised data access, so it preserves data confidentiality. Indeed, in asymmetric cryptography, the key that is used to encrypt the data differs from the key used to decrypt it. For this reason, asymmetric cryptography is more secure than symmetric cryptography, because it is not necessary to share a key to decrypt a message.[125]

Asymmetric cryptography allows the verification by the receiver of the provenance and integrity of the received message. The sender encrypts the data with her private key and sends both the encrypted message and its hash. The receiver decrypts the message with the sender's public key. If the result is identical to the hash, the recipient can be sure that the message originated from the sender and was not modified by third parties.[126]

Nicotra and Sarzana di S. Ippolito[127] argue that such signatures might be adopted in permissioned blockchains because they are closed networks with pre-identified participants (unlike in permissionless blockchains). The possibility to identify the signatory could determine the satisfaction of requisite (b). We think that this is plausible in B2B scenarios because businesses can have the economic capacity to equip themselves with such instruments. Moreover, it is more likely that the economic value of their transactions is higher than that of B2C transactions, so there is a greater need to adopt the written form in contracts.[128] The authors claim that these solutions could also meet

[123] The Report "Blockchain and digital identity" of the EU Blockchain Observatory and Forum, at page 23, assumes that «it is possible that blockchain (…) signatures could be considered eIDAS-conform, including potentially up to the highest level, by recognising blockchains within solutions managed by trust service providers». Similarly, Giuliano concludes that blockchain technology makes use of the technological components of the digital signature. However, in the lack of a trust service provider that certifies underlying identities, there is not any equivalence with handwritten signatures. See M. Giuliano, *La blockchain e gli smart contracts nell'innovazione del diritto del terzo millennio*, in *Diritto dell'informazione e dell'informatica*, 6, 2018,1021.

[124] Art. 26 of the e-IDAS Regulation.

[125] In symmetric cryptography, the encryption key coincides with the decryption key. In asymmetric cryptography, the sender encrypts the message with the recipient's public key. The recipient decrypts the message with her private key that is kept secret by the receiver.

[126] I. Bashir, *Mastering Blockchain,* cit., 203.

[127] M. Nicotra - F. Sarzana di Sant'Ippolito (eds.), *Diritto della blockchain, intelligenza artificiale e IoT*, Milano, 2018, 64.

[128] Szczerbowski observes that «parties usually prefer written form in contract of substantial economic value». See J.J. Szczerbowski, *Place of smart contracts in civil law. A few comments on form and interpretation*, in *Proceedings of the 12th Annual International Scientific Conference NEW TRENDS 2017*, available at *SSRN*.

requirement (c), e.g. through OTP tokens or biometric authentication.[129]
Lastly, requirement (d) requires controls over the integrity of signed data even after the subscription.[130] We think that the immutable nature of blockchain (thanks to distribution and concatenated hashes) combined with the use of asymmetric cryptography can ensure the detectability of any changes over time. Data are linked to hashes that uniquely represent such data. Every attempt of tampering would cause the change of the hash and the subsequent hashes in the chain.[131]
Simple electronic signatures and advanced electronic signatures shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.[132] Recital 49 of the e-IDAS Regulation entrusts the Member States to establish when electronic signatures are considered equivalent to handwritten signatures.
For instance, in Italy, the *Codice dell'Amministrazione Digitale* (CAD)[133] considers an electronic document to be in written form when the signatory signs it by using a digital signature, a qualified electronic signature, or an advanced electronic signature.[134] In addition, the same legal value is recognised to a document formed in accordance to the requirements set by the *Agenzia per l'Italia Digitale* (AGID)[135] pursuant to Art. 71 of the CAD, upon prior IT identification of its author, in such a way as to guarantee its security, integrity, and immutability and the fact that it is ascribable to the author, in a clear and unequivocal manner.
The digital signature is a qualified electronic signature which is peculiar to the Italian legal system, and that makes use of asymmetric cryptography. The advanced electronic signature is also considered equivalent to handwritten signature. Moreover, the AGID has recently set the guidelines,[136] pursuant to Art. 71 of the CAD, to sign electronic documents with the *Sistema Pubblico per la gestione dell'Identità Digitale di cittadini e imprese* (SPID).
SPID is the Italian electronic identification mean pursuant to Art. 6 of the e-IDAS

[129] M. Nicotra - F. Sarzana di Sant'Ippolito, *Diritto della blockchain,* cit., 64-65.

[130] S. Troiano, *Article 26. Requirements for advanced electronic signatures*, in A. Zaccaria - M. Schmidt Kessel - R. Schulze - A.M. Gambino (eds.), EU *eIDAS Regulation,* cit., 228.

[131] In its report "Legal and Regulatory Framework of Blockchains and Smart Contracts", 12, the UE Blockchain Observatory and Forum writes that blockchains would appear to meet the technical criteria of simple and advanced electronic signatures.

[132] Art. 25(1) of the e-IDAS Regulation.

[133] Legislative Decree 7 March 2005, no. 82.

[134] According to Art. 21(2) of the *CAD*, by contrast with Art. 20(1-*bis*), the juridical acts included in Art. 1350(1-12) of the *Codice Civile* are valid only if signed with a digital signature or a qualified signature. According to Art. 21(2-*ter*) of the CAD, every electronic notarial deed is valid if signed by the notary with a digital or qualified signature. The other involved parties sign the deed with a digital, qualified or advanced electronic signature, or with handwritten signature digitally acquired.

[135] The *Agenzia per l'Italia Digitale* is the technical agency of the Presidency of the Council of Ministers, whose main purpose is to guarantee the achievement of the objectives of the Italian digital agenda, and that contributes to the diffusion of information and communication technologies, to foster innovation and economic growth.

[136] «*Linee guida contenenti le regole tecniche per la sottoscrizione elettronica di documenti ai sensi dell'art. 20 del CAD*».

Regulation. The guidelines of the AGID state that signatories can only be natural persons[137] with a SPID digital identity level two or higher.[138] The service provider affixes its qualified electronic seal[139] to the document and sends it to the signatory's identity provider. After the signature with the SPID, the identity provider affixes its own qualified electronic seal.

On this point, Art. 8-*ter*(2) of the Italian *Decreto Semplificazioni,*[140] which has introduced some binding norms for blockchain-based smart contracts, states that smart contracts satisfy the requirement of the written form upon prior IT identification of the interested parties through a process that meets the requirements set by the AGID with guidelines. The Art. is very similar to Art. 20(1-*bis*) of the CAD where it recognises the same legal value of handwritten signatures to documents formed in accordance with the requirements set by the AGID pursuant to Art. 71 of the CAD. Indeed, the Determination of the General Director of the AGID no.116/2019 of 10 May 2019 – that has established a Working Group for the preparation of such guidelines and technical standards – provides that the guidelines have to be formed in accordance with the procedure set out in Art. 71 of the CAD and the Regulation for the adoption of Guidelines for the implementation of the CAD.[141] However, unlike Art. 20 of the CAD, the Simplification Decree generically refers to a process upon prior identification of the parties without setting any requirements (whose determination is left to the AGID). Moreover, because the article does not consider electronic signatures, Manente[142] wonders whether the AGID can also provide the use of digital, qualified, or advanced signatures in blockchain-based smart contracts.

In all other cases, the suitability of the document to satisfy the requirement of the writ-

[137] Both for non-professional and professional use (also representing a legal person).

[138] They are assurance levels. The first level is for transactions with a low degree of risk and requires a single-factor authentication system (e.g. a password). The second level is for transactions with a substantial degree of risk and requires a double-factor authentication system (e.g. a password and an OTP). The third level is for transactions with a high degree of risk and requires the use of double-factor authentication systems based on digital certificates and stored on devices that meet some security requirements set by Annex III of the Directive 1999/93/EC (now Annex II of the e-IDAS Regulation).

[139] Like qualified electronic signatures, qualified electronic seals are created by a qualified electronic seal creation device and are based on a qualified certificate for electronic seals (Art. 3(27) of the e-IDAS Regulation). Electronic seals are a novelty introduced by the e-IDAS Regulation. Like electronic signatures, electronic seals are data in electronic form, which is attached to or logically associated with other data in electronic form (Art. 3(25)). But, unlike electronic signatures, electronic seals can only be created by a legal person (Art. 3(24)) and do not have the function of certifying the consent of a legal person in relation to a statement. However, there are some member States where legal persons are enabled to use electronic signatures. So, moving from Recital 24, commentators observed that the Member States may introduce additional functions to electronic seals, thus recognising electronic seals as being the same as legal persons' signatures. To deepen these aspects, see S. Gatti, *Article 35. Legal effects of electronic seals*, in A. Zaccaria - M. Schmidt Kessel - R. Schulze - A.M. Gambino (eds.), EU *eIDAS Regulation,* cit., 276 ss.

[140] *Legge 11 febbraio 2019, n. 12, di conversione del decreto legge 14 dicembre 2018, n. 135, recante disposizioni urgenti in materia di sostegno e semplificazione per le imprese e la pubblica amministrazione* (Law no. 12 of 11 February 2019 converting Decree no. 135 of 14 December 2018).

[141] The Determination can be accessed at *trasparenza.agid.gov.it.*

[142] M. Manente, *L. 12/2019 – Smart contract e tecnologie basate su registri distribuiti – prime note, Studio 1_2019*, March 2019, 6.

ten form can be freely assessed in court, with respect to its characteristics of security, integrity, and immutability. Maybe, judges might consider that asymmetric cryptography, hash function, and decentralised databases guarantee the integrity and the immutability of the document. The greatest difficulty seems the fact that in permissionless blockchains the keys are not ascribable to precise identities. However, sometimes it could be possible to reconnect an account to an identified person.[143]

9. Conclusions

The study provided a legal analysis of the use of blockchain technology for the formation of smart legal contracts. It clarified that, despite the term, smart contracts are not necessarily contracts. Even when smart contracts are used in the contractual domain, the mere fact that a smart contract is stored on a blockchain does not give rise to a legal agreement. Indeed, the agreement constitutes the very basis of the contract. In the light of that, smart legal contracts can be concluded off-chain and on-chain. In the former case, smart contracts are mere tools for the automatic performance of the contract (or part of it). In the latter case, the smart contract represents, in combination with the blockchain, the tool through which the parties express their contractual will. Therefore, there was the need to verify how the rules on contract formation can be interpreted to make blockchain-based smart contracts fit into contract law.

To this end, the article took into consideration contract requirements. It started from the agreement, taking into account the exchange of offer and acceptance and the time of conclusion of the contract. Then, it investigated the contractual intention and the form of the contract. It also focused on information requirements and acknowledgment of receipt, that are not contract requirements but apply before or at the moment of placing an online order, so they concern contract formation. The analysis showed that existing general principles and rules of contract law can also be adapted to this new context. Basically, the questions are the same as in electronic commerce. For instance, the transition from paper documents and physical addresses to electronic documents and addresses; the use of non-standard ways and languages for making contract proposals; the issue of a lack of trust between the parties due to forms of distance communication; the difficulty of linking the contractual will to precise identities. As a consequence, analogous legal questions imply analogous legal solutions. For these reasons, it seems that, at least for contract formation, there is not the need to provide new *ad-hoc* rules.

[143] For instance, when the address appears on a personal webpage, blog, or forum. About the pseudonymous character of public keys in permissionless blockchain, and the techniques used to trace back to underlying identities, see P. De Filippi, *The interplay between decentralization and privacy: the case of blockchain technologies*, in *Journal of Peer Production*, 7, 14 September 2016, 11-13, available at *SSRN*; M. Finck, *Blockchains and Data Protection in the European Union*, in *European Data Protection Law Review*, 1, 2018, 22; J. Barcelo, *User Privacy in the Public Bitcoin Blockchain*, in *Journal of Latex Class Files*, 6, 2007, 1; A. Gambino - C. Bomprezzi, *Blockchain e protezione dei dati personali*, in *Diritto dell'informazione e dell'informatica*, 3, 2019, 633.