



MARIA FRANCESCA TOMMASINI

Professoressa ordinaria di Diritto privato – Università degli Studi di Messina

LO SMART CONTRACT E IL DIRITTO DEI CONTRATTI

SOMMARIO: 1. I sistemi di Intelligenza Artificiale applicati al settore giuridico. Lo smart contract. – 2. Individuazione della fattispecie e suo inquadramento giuridico. – 3. Lo smart contract in Italia. Lo smart contract con funzione “strumentale” e con funzione meramente “esecutiva”. – 4. Lo smart contract con funzione “costitutiva” del contratto. Formazione ed intelligibilità del documento. – 5. La forma elettronica e l’identificazione delle parti contraenti. Lo smart contract concluso da un terzo. – 6. Segue. La pseudonimizzazione dei dati e la loro tutela giuridica. – 7. Esecuzione del vincolo ed irretrattabilità dello smart contract. La funzione kill o selfdestruct code. – 8. Le patologie del contratto. La nullità dello smart contract. – 9. L’annullabilità dello smart contract. La rilevanza dei vizi del volere. – 10. Segue. Gli errori di progettazione o di programmazione. La responsabilità dei gestori per il malfunzionamento della blockchain. – 11. La risoluzione del contratto concluso mediante smart contract. La gestione delle sopravvenienze nei contratti di durata. – 12. Segue. La risoluzione di diritto. – 13. La rescissione. – 14. Foro competente e disciplina transnazionale per le controversie nascenti da smart contract. Il ricorso all’arbitrato. – 15. Rilievi conclusivi.

1. – Le opportunità offerte dalle nuove tecnologie stanno cambiando la vita di tutti¹. Ci si muove verso una realtà sempre più robotizzata, veloce, in cui le macchine sono in grado di operare in maniera intelligente arrivando ad emulare la mente umana e di sostituirsi in un numero considerevole di attività da sempre ritenute appannaggio degli uomini². La straordinaria novità dei sistemi robotici e di intelligenza artificiale (IA)³, è

¹ F. MAGGINO, G. CICERCHIA, *Algoritmi, etica e diritto*, in *Diritto inf. e dell’informatica* 2019, 6, 1161; S. CRISCI, *Intelligenza artificiale ed etica dell’algoritmo*, in *Foro amm.*, 2018, 10, 1787.

² Si pensi ad attività quali tradurre testi (B. MARR, *Will machine learning AI make human translators an endangered species?*, in *Forbes*, 2018), redigere articoli di attualità (M. MAGRINI, *La notizia robotizzata. Giornali e giornalismo davanti all’onda dell’intelligenza artificiale*, in *Problemi inf.*, 2017, 147), scrivere poesie (M. BURGESS, *Google’s AI has written some amazingly mournful poetry*, in *Wired UK* 2016), comporre musica (B. KALEAGASI, *A new AI can write music as well as a human composer*, in *Futurism* 2017), dipingere opere d’arte (G. COHN, *AI art at Christie’s sells for \$432,500*, in *New York Times digital edition*, 2018), ideare soluzioni a problemi tecnici (S. RAVID, X. LIU, *When Artificial Intelligence systems produce inventions: an alternative model for patent law at the 3A era*, in *Cardozo L. Rev.* 2018, 2215).

³ I sistemi di Intelligenza Artificiale, ipotizzati per la prima volta nel 1955 dal matematico John McCarthy, si distinguono tra sistemi di IA debole (*weak AI*) e IA forte (*strong AI*): la prima consiste in programmi matematici con cui si sviluppano funzionalità per il *problem solving* o per consentire alle macchine di prendere decisioni; sono, in altre parole, sistemi in grado di simulare specifiche funzionalità cognitive dell’uomo senza però raggiungere le complessive capacità intellettuali sue tipiche. L’IA debole si fonda, dunque, su metodi che consentono al software di apprendere in modo che le reti possano svolgere un compito senza che vi siano pattern indicati dall’esterno che stabiliscano come essa debba comportarsi o reagire, esattamente come accade per SIRI, l’assistente vocale di proprietà Apple Inc (T. ROTHKEGEL, M. TAYLOR, *What characterises Artificial Intelligence and how does it work?*, in *Computer and Telecommunications Law Review*, 2016, 98). L’IA forte, al contrario, ricomprende sistemi cosiddetti «autoscienti» capaci quindi di sviluppare una propria intelligenza senza emulare processi di pensiero o capacità cognitive simili all’uomo, ma sviluppandone una propria in modo autonomo (A. OTTOLIA, *Big Data e innovazione computazionale*, Torino, 2017,



quella di poter elaborare dati in maniera massiccia aggregandoli e disaggregandoli fra loro ad una velocità elevatissima, e di consentire al *software* di apprendere automaticamente da schemi secondo diversi modelli che vanno dal *neural network*⁴, al *machine learning*⁵; dal *deep learning*⁶ al *cognitive computing*⁷ e al *natural learning processing NLP*⁸. Le tecnologie intelligenti, verso la cui regolamentazione l'Unione Europea sta intervenendo con sempre maggiore decisione⁹, non si limitano ad automatizzare oggetti e città¹⁰, attività di

19). L'IA si riferisce dunque alla capacità delle macchine di svolgere compiti umani e replicare efficacemente parti della mente umana, studiando modelli di apprendimento ispirati alla struttura e al funzionamento del cervello biologico. Questi sistemi, già in uso nell'individuazione di schemi, nel riconoscimento vocale o delle immagini, utilizzano reti neurali artificiali progettate ad hoc (CNN e RNN).

⁴ Il *neural network* è un tipo di apprendimento automatico composto da unità interconnesse (come i neuroni) capace di elaborare le informazioni rispondendo a *input* esterni, trasmettendo informazioni tra ciascuna unità. Il processo richiede più passaggi ai dati per trovare connessioni e ottenere significati da dati non definiti.

⁵ Il *machine learning* automatizza la costruzione di modelli analitici utilizzando le *neural networks* e applicandoli in impieghi statistici, di ricerca operativa e fisica in modo da trovare collegamenti non evidenti nei dati, senza che vi sia stata una specifica programmazione sui contenuti e sui luoghi della ricerca. UN'IA che si avvale della tecnologia del *machine learning* è capace di ricevere una vasta quantità di dati al fine di comprenderne ed elaborarne il contenuto. UN'IA di questo tipo può istruire ed aggiornare l'algoritmo con cui opera sia grazie all'apprendimento automatico sia in virtù dell'analisi delle informazioni che le vengono fornite.

⁶ Il sistema di *deep learning* utilizza enormi reti neurali con molti strati di unità di elaborazione, sfruttando i progressi della potenza di calcolo e tecniche di addestramento migliorate per apprendere schemi complessi in grandi quantità di dati. Le applicazioni comuni includono il riconoscimento di immagini e voce.

⁷ Il *cognitive computing* è fondato sulla ricerca di un'interazione naturale e umana con le macchine. Usando L'IA e il *cognitive computing*, l'obiettivo finale è che una macchina simuli i processi umani attraverso la capacità di interpretare immagini e linguaggio, e quindi parli in modo coerente in risposta.

⁸ Il *natural learning processing NLP* consiste nella capacità dei computer di analizzare, comprendere e generare il linguaggio umano. La fase successiva del NLP è l'interazione del linguaggio naturale, che consente agli esseri umani di comunicare con i computer utilizzando il normale linguaggio quotidiano per svolgere attività.

⁹ Il più recente intervento in Europa sul tema è il Progetto di relazione recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale [2020/2014 (INL)]. Il progetto è alla base della Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale [2020/2014 (INL)]. Il Parlamento UE ha giocato di anticipo ed ha approvato il 20 ottobre 2020 tre Risoluzioni con specifiche richieste in ordine alla futura normazione più altri testi meno specifici ma ugualmente assertivi tra cui quello sull'utilizzo di A.I. nel sistema penale. Ha adottato tre proposte che precisano come l'UE possa regolamentare l'intelligenza artificiale più efficacemente per dare una spinta positiva all'innovazione, agli standard etici e alla fiducia nella tecnologia. La prima risoluzione (A9-0186/2020) affronta il tema, potremmo dire "costituzionale", dei presidi etici che le applicazioni di intelligenza artificiale dovranno garantire per assicurare sicurezza, trasparenza e presa di responsabilità, ed evitare la creazione di pregiudizi e di discriminazioni, stimolare la responsabilità sociale e ambientale e come assicurare il rispetto dei diritti fondamentali. La seconda A9-0178/2020 riguarda il tema sensibile del regime della responsabilità civile per danni e pregiudizi arrecati da sistemi di A.I. La terza risoluzione (A9-0176/2020) riguarda i diritti di proprietà intellettuale, nella quale il Parlamento ha ribadito l'importanza di avere un sistema efficace per un ulteriore sviluppo dell'intelligenza artificiale, tra cui il rilascio di licenze e nuovi processi creativi. Questi interventi sono stati preceduti dalla Risoluzione del Parlamento Europeo, datata 12 febbraio 2019, Una politica industriale europea globale in materia di robotica e intelligenza artificiale, in *G.U.U.E.* C449/37 del 23 dicembre 2020; dalla Comunicazione della Commissione Europea al Parlamento, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni "L'intelligenza artificiale per l'Europa" del 25 aprile 2018, doc. n. COM (2018) 237 che ha definito l'Intelligenza artificiale come quei "sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi"; dalla Comunicazione del 7 dicembre 2018, COM (2018) 795; Building Trust in Human-Centric Artificial Intelligenc, 8 aprile 2019, COM (2019) 168 (Piano coordinato sull'intelligenza artificiale).

¹⁰ Si pensi allo "smartphone", letteralmente "telefono intelligente" o con funzionalità evolute, è un apparecchio che racchiude in sé sia le funzioni di un computer palmare che quelle di un telefono cellulare, con possibilità di personalizzazione con nuove funzioni e programmi. Sempre più spesso si sente poi parlare di smart watch (orologi con funzionalità evolute che possono andare dalla riproduzione di radio FM, audio, e file video attraverso un auricolare Bluetooth, alla possibilità di effettuare o rispondere alle chiamate), di smart TV, smart work, e ancora smart city, smart economy e persino smart governance, dove "smart" racchiude i concetti di migliore qualità di vita e minor impatto ambientale, grazie all'utilizzo intelligente delle tecnologie.



pubblico interesse¹¹ e settori cruciali del nostro ordinamento¹², ma affrontano e risolvono anche problemi legati ai processi di *business*, rendendo più veloci le decisioni e permettendo ai soggetti (persone fisiche e/o giuridiche) di essere più informati e precisi nella definizione delle operazioni commerciali. Si pensi alle ipotesi dei *data oriented contracts*¹³, dei *computable contract*¹⁴, dei *Ricardian contracts*¹⁵ e dei più recenti *smart contracts* i quali consentono di processare i dati più velocemente e di automatizzare operazioni che prima potevano svolgersi solo manualmente. È evidente l'impatto dirompente che tale tecnologia potrebbe avere sul mondo economico e, quindi, sulla regolamentazione dei nuovi rapporti giuridici, viepiù considerando che manca in materia una disciplina specifica ed uniforme.

¹¹ La tecnologia intelligente può essere utilizzata dalle pubbliche amministrazioni per la gestione dei sussidi e finanziamenti pubblici oppure per la gestione del sistema pensionistico, ovvero ancora per l'emissione, trasferimento, circolazione dei titoli di Stato e finanche per i procedimenti ad evidenza pubblica (S. CALDARELLI, *L'uso della tecnologia blockchain nel settore delle pubbliche amministrazioni: tra "mito" e realtà giuridica*, in *Dir. inf. e inform.* 2020, II, 4, 857).

¹² Nel settore giuridico i sistemi di IA coinvolgono talune specifiche aree di interesse ed in particolare il sistema per l'analisi giuridica per la sussunzione di un caso giuridico all'interno di una precisa fattispecie legale; il sistema per la pianificazione giuridica che suggerisce le azioni migliori per raggiungere un determinato risultato; il sistema per la ricerca di informazioni giuridiche che consente di cercare informazioni di contenuto concettuale-giuridico; il sistema della giustizia predittiva che sfrutta la capacità di sfruttare degli algoritmi di IA per predire l'esito dei giudizi (S. CRISCI, *Intelligenza artificiale ed etica dell'algoritmo*, in *Foro amm.*, 2018, 10, 1787). Nel "servizio Giustizia" (*smart judgement*), poi, ci si avvale dell'Intelligenza Artificiale robotica per dare esecuzione automatica alle sentenze, o per procedere alla sottrazione automatica di una somma cui si è stati condannati direttamente dal conto corrente oppure alla preclusione all'accesso dell'abitazione ove se ne accerti, attraverso un protocollo di *blocks*, che essa è di proprietà altrui (A.M. GAMBINO, *Vizi e virtù del diritto computazionale*, in *Dir. inf. e inform.*, 2019, II, 6, 1169). Non di meno, gli strumenti di IA sono utilizzati a livello diagnostico e terapeutico nell'attività medico sanitaria. L'evoluzione tecnologica, specie quella collegata al *cloud computing*, evidenzia come l'intera gestione del dato diagnostico e terapeutico, articolata secondo una successione cronologica predefinita di scansioni computazionali e di indicizzazione dei dati nosografici, reclama adeguata tutela (A. MARCHESE, *Profili civili- stici dell'infomation technology in ambito sanitario*, Napoli, 2021, 153 ss.).

¹³ I *data oriented contracts* sono accordi nei quali il contenuto è, in tutto o in parte, espresso in modo tale da risultare processabile da un *computer*, o perché direttamente redatto in linguaggio formale o perché frutto della traduzione di un testo contrattuale originariamente redatto in linguaggio naturale (M.J. RADIN, *Regulation by contract, regulation by machine*, in *Journal of Institutional and Theoretical Economics (JITE) / Zeitschrift für die gesamte Staatswissenschaft* 2004, 1, 142; M.L. PERUGINI, P. DAL CHECCO, *Introduzione agli smart contracts*, in <http://ssrn.com/abstract>). Nella scrittura di questi contratti le parti contraenti, da sole o con la collaborazione di un terzo programmatore, possono riferirsi sia a *standard* semantici già esistenti ovvero stipulare degli accordi preliminari – c.d. *data meaning threshold agreements* – nei quali indicare come termini ed espressioni devono essere intesi una volta tradotti in linguaggio formalizzato, procedendo ad una pre-attribuzione di significato, condivisa dai futuri contraenti, così che si possa istituire un collegamento tra voluto delle parti e sua rappresentazioni a fini di comprensione da parte di un *computer*. Il computer viene messo in condizione di comprendere il linguaggio ordinario attraverso *softwares ad hoc* mediante i quali le espressioni venivano trasformate in "dati".

¹⁴ I *computable contracts* sono accordi tra le parti rappresentati, in tutto o in parte, in codice binario. Nascono in codice, si potrebbe dire. Poiché sono nati in codice, permettono una serie di analisi, man mano che si raccolgono i dati in essi contenuti, esattamente come accade in tutti i "derivati" di internet (Big Data e Data analys). Questo permette la visualizzazione di relazioni economiche o giuridiche tramite dei *graphi* (grafici) che raccontano "dove va" il mondo degli affari (si parla al momento di contratti BtB o BtC di servizio o prodotto). E ancora. Sempre poiché sono contratti "nati" in codice, permettono una serie di azioni automatizzate che si verificano nella logica *if-then-else*; per esempio come gli *smart legal contracts* e non solo. Il contratto – insomma – si contra, si redige in linguaggio binario e si auto esegue automaticamente (C. AMATO, *La 'computerizzazione' del contratto (Smart, data oriented, computable e self-driving contracts. Una panoramica)*, in *Europa dir. priv.*, 2020, 4, 1259; H. SURDEN, *Computable contracts*, in *UC Davis Law Review*, 2012, 46).

¹⁵ I *Ricardian contracts* prendono il nome da David Ricardo in onore del suo contributo alla teoria del commercio internazionale. Ideati nel 1996 da Ian Grigg, essi si caratterizzano per la presenza di un *design pattern* che consente l'individuazione delle intenzioni delle parti prima che il contratto venga eseguito. Attraverso un processo detto "*prose, parameters and code*" la prosa legale viene legata al codice informatico per mezzo di parametri al fine di consentirne l'automazione. Essendovi una prosa legale i *Ricardian contracts* hanno validità giuridica e sono vincolanti per le parti. Una volta tradotti in codice informatico possono essere letti ed eseguiti anche dal computer. In altri termini il *Ricardian contract* sigla l'accordo tra le parti e ne consente la successiva esecuzione da parte della macchina.



2. – Pur traducendosi letteralmente come “contratti intelligenti”, la natura giuridica degli *smart contract* è stata oggetto di vivace dibattito. Mentre secondo alcuni autori, in considerazione della definizione data in origine dal suo ideatore¹⁶, lo *smart contract* si sostanzia in “un complesso di promesse, seppure in forma digitale, compresi i protocolli all’interno dei quali le parti adempiono automaticamente a tali promesse”¹⁷, ovvero in “un documento automatizzato”¹⁸; secondo altri, invece, esso consiste esclusivamente in un insieme di protocolli automatizzati e si struttura secondo un registro logico molto semplice, per cui al verificarsi di una certa condizione matematicamente accertabile (*if this ...*) si produce l’evento digitalmente collegato (*... then that*). Esso, di conseguenza, può assolvere funzioni semplici, come il pagamento in moneta digitale o la gestione di una procedura di voto, o complesse, quale la formazione di accordi giuridicamente vincolanti¹⁹. Di qui la considerazione che lo *smart contract* non può farsi rientrare nella accezione tradizionale di contratto²⁰. La dottrina fonda il proprio convincimento sulla definizione di cui al paragrafo 4.3 della Risoluzione del Parlamento Europeo del 16 febbraio 2017²¹, secondo cui lo *smart contract* può considerarsi uno strumento tecnologicamente avanzato che, utilizzando la DLT (*distributed ledger technology*)²² ed in particolare la *blockchain*²³, permette di realizzare un processo negoziale capace di eseguirsi in modo autonomo.

In una posizione intermedia tra chi riconosce allo *smart contract* la natura giuridica di contratto e chi, in-

¹⁶ Lo *smart contract* è frutto degli studi del giurista ed informatico statunitense N. SZABO, *Smart Contracts: Building Blocks for Digital Markets*, 1996, in <http://www.fon.hum.uva.nl/rob/Courses>. L’autore sostiene che lo *smart contract* è “a set of promises, specified in digital form including protocols within which the parties perform on the these promises”. Queste poche parole sono precedute da una apparente spiegazione: “New institutions, and new ways to formalize the relationships that make up these institutions, are now made possible by the digital revolution. I call these new contracts “smart”, because they are far more functional than their inanimate paper-based ancestors”. Szabo non indica specificamente a quali istituti e a quali modi di formalizzare le relazioni faccia riferimento, ma si intuisce che pensasse a soluzioni criptografiche idonee a conferire ai documenti informatici eguale valore costitutivo e probatorio dei tradizionali documenti cartacei.

¹⁷ S. GEORGE, *Smart contracts: tools for transactional lawyers*, in *Texas J.B.*, 2018, 404; W. CHEN, *Law*, Oxford, 2018, 71; A. BLUM, *Contracts*, New York, 2007, 2 secondo cui lo *smart contract* non è inquadrabile né quale “promise or agreement recognized by the law” né quale “exchange relationship created by oral or written agreement between two or more persons, containing at least one promise, and recognized in law as enforceable”.

¹⁸ H. SURDEN, *Computable Contracts*, in *U.C. Davis L. Review*, 2012, 629; K. WERBACH, N. CORNELL, *Contracts Ex Machina*, in *Duke L. J.*, 2017, 338.

¹⁹ M. GIULIANO, *La blockchain e gli smart contracts nell’innovazione del diritto nel terzo millennio*, in *Dir. inf. e inform.*, 2018, II, (II), 989.

²⁰ In proposito, si vedano: P. SIRENA, *Le questioni degli smart contract con riguardo alla struttura ed alla patologia del contratto. Intervento al Convegno Il robot tra diritto e processo*, Roma 21 febbraio 2019; E. GABRIELLI, *La nozione di contratto e la sua funzione. Appunti sulla prospettiva di una nuova definizione di contratto*, in *Giust. civ.*, 2019, 2, 299. Dello stesso avviso è anche F. DI CIOMMO, *Smart contracts and (non) law. the case of the financial markets*, in *Law and economics yearly review*, 2018, II, 291 ss. L’Autore si riferisce nello specifico alle operazioni nel settore dell’High Frequency Trading (HFT) e del c.d. algorithmic trading, entrambi da tempo “an established reality”. Secondo l’autore “*smart contracts are not contracts*”, e “any attempt made by jurists to understand and regulate the phenomenon risks becoming obsolete at the very moment is carried out”.

²¹ Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, in *G.U.U.E.* del 18 luglio 2018 (C 252/239).

²² La DLT è una tecnologia basata su registri distribuiti quali tecnologie e protocolli informatici che usano un registro condiviso, distribuito, replicabile e accessibile simultaneamente, architetture decentralizzate su basi crittografiche, tali da consentire la registrazione, la convalida, l’aggiornamento e l’archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili. Non tutti i registri distribuiti, però, sono costituiti da una catena di blocchi: ve ne sono anche alcuni basati su architetture decisamente differenti, come ad esempio *Tangle* che è basato su grafici aciclici. Dalle DLT si devono nettamente distinguere le c.d. *tecnologie basate su registri centralizzati* che si servono di database centralizzati nei quali inserire tutti i dati; gli utenti accedono al sistema (detto *client-server*) accettando le regole stabilite dall’amministratore centrale, al quale spetta, dunque, in piena autonomia, la gestione di ogni istanza e l’eventuale risoluzione di ogni controversia. Ove si rendano necessarie modifiche, sarà sempre il gestore a decidere se e come apportarle e, conseguentemente, l’utente ha la scelta se accettarle e, quindi, giovare di un nuovo servizio, ovvero rifiutarle con conseguente uscita dal sistema.



vece, la nega decisamente, si collocano coloro i quali ritengono utile distinguere nello *smart contract* due profili: uno detto “*smart code*” che consiste nella componente tecnica (programma informatico) che rende tale strumento soggetto alla disciplina relativa alla tutela del software²⁴, e l’altro, detto “*smart legal contract*” che è, invece, l’accordo vero e proprio operante su tecnologia blockchain ed al quale si attribuisce significato ed efficacia negoziale²⁵. Il profilo tecnico-informatico (*smart code*) assume un ruolo imprescindibile, perché consente di determinare l’identità e la natura dell’accordo così perfezionatosi (*smart legal contract*)²⁶. Questo orientamento, però, non convince pienamente poiché finisce per limitare l’analisi dello

²³ La Blockchain (letteralmente catene di blocchi) si sostanzia in una tecnologia di registri distribuiti (o codici) in cui i dati delle transazioni vengono memorizzati su singoli nodi costituenti la catena, gli uni connessi agli altri, attraverso un processo di comunicazione simile alle reti *peer to peer*. Ciò implica che per potere modificare una singola parte della catena è necessario ottenere il consenso di tutti gli altri nodi (sul punto si vedano: P. BOUCHER, *Come la tecnologia blockchain può cambiarci la vita*, in *Servizio di ricerca del Parlamento Europeo*, 2017, 4; S. CRISCI, *Intelligenza artificiale ed etica dell’algoritmo*, in *Foro amm.*, 2017, 10, 1787 ss.; M. IANSITI, K. LAKHANIR., *The truth about Blockchain*, in *Harvard Business Review*, 2017; C. MILLARD, *Blockchain and law: incompatible codes?*, in *Computer Law & Security Review*, 2018, 843 ss.). Il sistema blockchain può essere di tipo pubblico (*permissionless*), privato (*permissioned*) e a permesso condiviso (*consortium*). Nel primo caso, qualunque utente può contribuire all’aggiunta e all’aggiornamento dei blocchi e disporre delle copie di quanto viene approvato. Tra le più importanti blockchain pubbliche ci sono Bitcoin ed Ethereum. Il sistema Bitcoin (BTC) è stato progettato per inviare denaro in tutta sicurezza su Internet, senza necessità di intermediazione del sistema bancario e senza timori di frodi, e il suo linguaggio di programmazione, volutamente limitato per garantire una maggiore sicurezza, non consente di inviare grande quantità di dati per ogni transazione né di eseguire calcoli oltre a quelli necessari per eseguire una transazione. Ethereum (ETH) è, invece, una piattaforma decentralizzata che può essere scaricata gratuitamente e ha la capacità di essere programmata, similmente ad un computer (G. GITTI, *Emissione e circolazione di criptoattività tra tipicità e atipicità dei nuovi mercati finanziari*, in *Banca, borsa e tit. cred.*, 2020, 1, 13; G. GITTI, M. MAUGERI, C. FERRARA, *Offerte iniziali e scambi di cripto attività*, in *Oss. dir. civ. e comm.*, 2019, 1, 103; F. BARTOLINI, *Requisiti della criptovaluta, ex articolo 2464, comma 2, c.c. ai fini del conferimento nel capitale sociale di una s.r.l.*, in *IlSocietario.it*, 2018). Nel caso della blockchain privata (*permissioned*) soltanto un numero limitato di nodi, detti *trusted*, può svolgere operazioni di aggiunta o aggiornamento dei blocchi, giacché in questa tipologia di blockchain vi è l’esigenza di limitare queste operazioni soltanto a coloro in possesso di una specifica autorizzazione. Ad utilizzare la tipologia di tipo privato sono in larga parte operatori economici, quali, ad esempio, compagnie aeree, società internazionali di distribuzione alimentare, compagnie energetiche, che hanno un ruolo evidentemente strategico nel mercato internazionale. Si pensi, tra gli altri, ai sistemi blockchain di tipo privato creati da British Airways per la risoluzione delle problematiche legate all’organizzazione dei voli commerciali, da UPS per la tracciabilità e la spedizione delle merci, da Walmart per la sicurezza dei prodotti alimentari o da Shell per la distribuzione di energia (G. FINOCCHIARO, C. BOMPRESZI, *A legale analysis of the use of blockchain technology for the formation of smart legal contract*, in *MediaLaws*, 2020). La blockchain del tipo “*consortium*” o a “permesso condiviso” o “parzialmente decentralizzata” è caratterizzata dal fatto che il processo di consenso è controllato da un insieme preselezionato di nodi che svolgono la funzione di validatori. Esempi di tale tipo blockchain è il consorzio R3 CEV LLC, una società finanziaria e di ricerca tecnologica che coopera con un consorzio di 200 società finanziarie (tra cui Banca d’America, Goldman Sachs, Citigroup, Banca Nazionale dell’Australia, Royal Bank del Canada, Sumitomo Mitsui Banking Corporation e altri) nello sviluppo dell’utilizzo della tecnologia blockchain all’interno del sistema finanziario. Altro progetto del tipo consorzio è Hyperledger, un progetto della Fondazione Linux che si basa su una blockchain con codice open source per supportare lo sviluppo collaborativo di registri distribuiti sulla base della blockchain. Cisco, Hitachi, IBM, Intel, NEC, J.P. Morgan, SAP e altri figurano tra coloro che vi hanno preso parte (N. ABRIANI, *Il diritto societario incontra il diritto dell’informazione. IT, corporate governance e corporate social responsibility*, in *Riv. soc.*, 2020, 1326).

²⁴ Nell’ordinamento italiano la tutela del software segue la legge sul diritto di autore (l. n. 633/1941), emendata proprio per disciplinare anche le produzioni dell’arte e dell’ingegno rese possibili dall’evoluzione tecnologica. In particolare, la normativa in vigore tutela i programmi e i codici che ne rendono possibile lo sviluppo. Si parla dunque di titolarità di diritti d’autore sul software, non già di diritti di proprietà; del software si protegge la forma (stringhe di codici) con cui il programma si esprime, quindi divenendo fruibile. L’art. 2 n. 8 della l. n. 633/1941 dispone che sono compresi nella protezione “i programmi per elaboratore, in qualsiasi forma espressi purché originali quale risultato di creazione intellettuale dell’autore. Restano esclusi dalla tutela accordata dalla presente legge le idee e i principi che stanno alla base di qualsiasi elemento di un programma, compresi quelli alla base delle sue interfacce. Il termine programma comprende anche il materiale preparatorio per la progettazione del programma stesso”.

²⁵ S. RIGAZIO, *Smart contracts e tecnologie basate su registri distribuiti nella l. 12/2019*, in *Dir. inf. e inform.*, 2021, 2, 369.

²⁶ Sul rapporto tra fase di esecuzione dello *smart contract* e fase di perfezionamento dello stesso si vedano: M. DUROVIC, A. JANSSEN, *The formation of smart contracts and beyond: shaking the fundamentals of contract law?*, in *Smart contracts and block-*



smart legal code proprio alla fase di perfezionamento del contratto, tralasciando di considerare il momento esecutivo-applicativo che, invece, negli *smart contract* risulta peculiare. La nostra indagine, perciò, si concentrerà sia sul profilo della formazione dell'accordo, con uno sguardo agli elementi essenziali propri del contratto tradizionale, che su quello della efficacia dello *smart contract*. La valorizzazione di entrambi i profili sarà volta, in special modo, a verificare l'eventuale compatibilità dell'accordo sviluppatosi su tecnologia blockchain con la nozione tradizionale di contratto²⁷. Le categorie concettuali classiche, infatti, dinnanzi alle nuove tecnologie, non devono necessariamente essere considerate un *a priori* ma vanno verificate²⁸, talvolta adattate, e possono rappresentare uno strumento di passaggio per pervenire "ad un risultato plausibile"²⁹. E laddove lo strumentario giuridico esistente si riveli insufficiente a disciplinare nuove forme di relazioni, specie se ci si trovi di fronte a paradigmi del tutto nuovi, come nel caso dei rapporti dematerializzati eseguiti in una rete, in cui, oltre ai beni, è la stessa persona ad assumere un'identità virtuale³⁰, sarà compito del legislatore adottare le più opportune soluzioni affinché l'individuo possa esplicare la propria attività in un contesto comunque garantito e regolato³¹.

chain technology: role of contract law, Cambridge, 2019; M. DUROVIC, F. LECH, *The enforceability of smart contracts*, in *The italian law journal*, 2019, 493.

²⁷ In dottrina la questione della compatibilità con le tradizionali categorie dogmatiche del contratto era già stata affrontata con riferimento al commercio elettronico e, nello specifico, al contratto telematico (G. PERLINGERI, F. LAZZARELLI, *Il contratto telematico*, in AA.VV., *Manuale del diritto dell'informatica*, Napoli, 2016; F. SGUERSO, *Il contratto telematico. Le moderne tecnologie e il "vecchio" codice civile*, in www.aicsweb.it/documenti/2012; E. TOSI, *Il contratto virtuale*, in *Studium juris*, 2008, 67; A.M. GAMBINO, *L'accordo telematico*, Milano, 1997, 11; V. ZENO-ZENCOVICH, *Sul rilievo pratico o sistematico della categoria dei c.d. contratti di informatica*, in AA.VV., *I contratti di informatica. Profili civilistici, tributari e di bilancio*, a cura di ALPA-ZENO ZENCOVICH, Milano, 1987, 32; F. GALGANO, *La cultura giuridica italiana di fronte ai problemi informatici (considerazioni di sintesi)*, in AA.VV., *I contratti di informatica. Profili civilistici, tributari e di bilancio*, cit., 373. Anche in quell'occasione, infatti, in un primo momento la dimensione tecnico-informatica aveva messo fortemente in discussione aspetti fondamentali quali la conclusione e l'esecuzione del contratto; tuttavia con un'attenta riflessione incentrata sulla funzione che lo strumento informatico svolgeva in tale contesto, la dottrina aveva recuperato e ritrovato le categorie civilistiche tradizionali nella nuova realtà telematica, interpretando i bisogni e gli interessi che andavano emergendo e che richiedevano tutela da parte dell'ordinamento (P. SAMMARCO, *I nuovi contratti dell'informatica. Sistema e prassi*, in *Trattato di diritto commerciale e di diritto pubblico dell'economia*, diretto da F. GALGANO, Padova, 2006; L. FOLLIERI, *Il contratto concluso in Internet*, Napoli, 2005; C. SCOGNAMIGLIO, *La conclusione e l'esecuzione del contratto telematico*, in AA.VV., *Commercio elettronico e categorie civilistiche*, Milano, 2002, 73; F. DELFINI, *Contratto telematico e commercio elettronico*, Milano, 2002; C. CAMARDI, *Contratto e rapporto nelle reti telematiche. Un nuovo modello di scambio*, in *Contratto e impresa* 2001, 2, 557; S. GIOVA, *La conclusione del contratto via Internet*, Napoli, 2000; E. GIANNANTONIO, *Manuale di diritto dell'informatica*, Padova, 1994; V. FRANCESCHELLI, *Computer e diritto*, Rimini, 1989).

²⁸ Sul progresso tecnologico e sulle sue ricadute sul piano giuridico si vedano: G. CORASANITI, *Il diritto nella società digitale*, Milano, 2018; N. IRTI, E. SEVERINO, *Dialogo su diritto e tecnica*, Roma-Bari, 2001; V. FROSINI, *Il diritto nella società tecnologica*, Milano, 1981, 202.

²⁹ N. LIPARI, *Le categorie del diritto civile*, Milano, 2013, 33.

³⁰ U. GALIMBERTI, *Psiche e techne. L'uomo nell'età della tecnica*, Milano, 1999, 12, secondo cui "noi continuiamo a pensare la tecnica come uno strumento a nostra disposizione, mentre la tecnica è diventata l'ambiente che ci circonda e ci costituisce secondo quelle regole di razionalità che, misurandosi sui soli criteri della funzionalità ed efficienza, non esitano a subordinare le esigenze dell'uomo alle esigenze dell'apparato tecnico". Ne risultano così rivisti "i concetti di individuo, identità, libertà, spazio, tempo di cui si nutrivano l'età umanistica e che ora, nell'età della tecnica, dovranno essere riconsiderati, dismessi o rifondati alle radici".

³¹ M. GIULIANO, *La blockchain e gli smart contracts nell'innovazione del diritto nel terzo millennio*, cit., 989. In questo senso anche G. DI ROSA, *Quali regole per i sistemi automatizzati "intelligenti"?*, in *Riv. dir. civ.*, 2021, 5, 826, secondo cui "occorre in primo luogo individuare gli ordini di conflitti a cui dà luogo l'utilizzo di robot, anche in considerazione della relativa differenziazione in termini di catalogazione identificativa; riportare, poi, le questioni così evidenziate con le regole date; saggiare, infine, la (eventuale) riferibilità (o, comunque, adattabilità) e, dunque, la possibile applicazione di regolamentazioni (già) sussistenti alle specifiche problematiche del settore indagato. In alternativa ... si tratta di provvedere alla predisposizione di nuove discipline, appropriate in ragione della specificità e della particolarità delle questioni sollevate".



3. – Sulla spinta della normativa europea³² ed extraeuropea³³, l'Italia è stato uno dei primi paesi dell'Unione³⁴ a riconoscere lo stato giuridico dello *smart contract* definendolo come “un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o

³² Sul piano legislativo un particolare cenno merita la Risoluzione del Parlamento europeo del 13 gennaio 2020 rubricata “Tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione”, in <https://www.europarl.europa.eu>, che prende in esame la tecnologia blockchain e, più in generale, l'insieme delle tecnologie basate su registri distribuiti (Distributed Ledger Technology – DLT), analizzandone le possibili applicazioni e fornendo indicazioni alla Commissione europea e alle altre istituzioni dell'Unione. Di poco successiva, del 20 ottobre 2020 è la Risoluzione del Parlamento Europeo sui servizi digitali: migliorare il funzionamento del mercato unico, in *G.U.U.E. C404/2* del 6 ottobre 2021, in cui il Parlamento ritiene che, nella regolamentazione degli aspetti civili e commerciali delle DLT e degli Smart Contracts, si debbano prevedere “misure che garantiscano l'esistenza di un adeguato quadro normativo per lo sviluppo e la diffusione dei servizi digitali, fra cui tecnologie di registro distribuito come le blockchain e i contratti intelligenti; misure atte ad assicurare che i contratti intelligenti siano dotati di meccanismi in grado di arrestarne e invertirne l'esecuzione, in particolare alla luce delle preoccupazioni private della parte debole o delle preoccupazioni pubbliche, per esempio quelle legate agli accordi di cartello e ai diritti dei creditori in caso di insolvenza e ristrutturazione; misure che garantiscano equilibrio e parità adeguati tra le parti per quanto riguarda i contratti intelligenti, tenendo conto in particolare degli interessi delle piccole imprese e delle PMI, per le quali la Commissione dovrebbe prendere in esame le possibili modalità; un aggiornamento del documento di orientamento esistente relativo alla direttiva 2011/83/UE, al fine di chiarire se i contratti intelligenti siano contemplati dall'eccezione di cui all'articolo 3, paragrafo 3, lettera i), della succitata direttiva, e di chiarire le questioni legate alle transazioni transfrontaliere, ai requisiti di certificazione notarile e al diritto di recesso” (sul punto si veda M. MAUGERI, *La Risoluzione del Parlamento europeo del 20 ottobre 2020 sugli smart Contracts nella prospettiva del diritto dei contratti e della concorrenza*, in *Contr. impr. Eu.*, 2021, 25 ss.). La Commissione Europea il 24 settembre 2020 ha presentato una proposta di direttiva in tema di crypto-assets che si inserisce nel più generale ambito della finanza digitale con specifica attenzione rivolta proprio all'utilizzo delle tecnologie DLT e blockchain in quest'ambito. La proposta suggerisce che, nell'affrontare le questioni derivanti dall'utilizzo di questi strumenti, le istituzioni comunitarie devono prediligere un approccio improntato alla cautela e, se del caso, all'adozione di strumenti di *soft law* e *best practices* (S. RIGAZIO, *Smart contracts e tecnologie basate su registri distribuiti nella l. 12/2019*, in *Dir. inf. e inform.*, 2021, 2, 369).

A livello europeo rileva, altresì, l'istituzione da parte della Commissione europea dell'*EU Blockchain Observatory and Forum* il 1° febbraio 2018 e dell'*European Blockchain Partnership* il 10 aprile 2018. *ALL'EU Blockchain Observatory and Forum* è attribuito il compito di raccogliere informazioni, mappare le principali iniziative esistenti, monitorare gli sviluppi e analizzare le tendenze, esaminare il potenziale socio-economico e affrontare le sfide, cercando di garantire un approccio uniforme e comune a livello europeo. L'*EU Blockchain Observatory and Forum* ha istituito due gruppi di lavoro per identificare e ricercare le iniziative esistenti basate su blockchain: *The Blockchain Policy and Framework Conditions Working Group*, deputato a definire le condizioni politiche, legali e regolamentari necessarie per la diffusione su larga scala delle applicazioni basate sulla blockchain, e *The Use Cases and Transition Scenarios Working Group*, chiamato a concentrarsi sui casi di utilizzo più promettenti, con particolare attenzione alle applicazioni del settore pubblico come identità e servizi pubblici, assistenza sanitaria, energia e rendicontazione ambientale. L'*European Blockchain Partnership* mira, invece, a consolidare il ruolo dell'Europa nello sviluppo e nella diffusione della tecnologia blockchain per mezzo di un approccio uniforme a livello europeo; a tale scopo i rappresentanti dei Paesi partecipanti lavorano insieme, al fine di stabilire le linee di intervento utili per sfruttare il potenziale dei servizi basati sulla blockchain a beneficio dei cittadini, della società e dell'economia. Tra queste iniziative, il partenariato sta cooperando per la creazione dell'*European Blockchain Services Infrastructure* (EBSI), capace di supportare la fornitura di servizi pubblici transfrontalieri in tutta l'Unione Europea, utilizzando la tecnologia blockchain e garantendo alti standard di sicurezza e protezione dei dati personali (F. FAINI, *Blockchain e diritto: la “catena del valore” tra documenti informatici, smart contracts e data protection*, in *Resp. civ. prev.*, 2020, 1, 297).

³³ Nel Regno Unito è stata istituita la *UK Jurisdiction Taskforce* (UKJT) che, il 9 maggio 2019, ha attivato una consultazione conclusasi il 31 marzo 2021 per definire e rendere pubblico l'orientamento del Governo nell'ambito delle nuove tecnologie e dello *smart contract*. La UKJT ha sostenuto la fattibilità, giuridica e informatica di *smart contract* con rilevanza contrattuale e conseguente applicazione del diritto dei contratti. Essa ha, inoltre, precisato che lo *smart legal contract* è una sottocategoria degli *smart contract* che è, o è parte di, un contratto tradizionale. La UKJT propone una tripartizione degli *smart legal contract* in tre categorie. La prima è quella del *Solely code model* che è espresso solo in codice informatico; la seconda categoria detta *Internal Model* che è un documento scritto contemporaneamente in linguaggio umano e in codice informatico in modo da essere comprensibile sia dalle parti che dalla macchina; la terza categoria è quella del *External Model* che consiste in un contratto tradizionale, ossia redatto interamente in linguaggio naturale, che include l'accordo delle parti a gestire l'esecuzione di alcune disposizioni con *smart contract*. Sulla base del lavoro compiuto dalla UKJT, la Law Commission ha definito gli *smart contract* come “legally binding contracts in which some or all of the contractual obligations are recorded in or performed automatically by a computer program” (in <https://www.lawsociety.org.uk/support-services/lawtech>).



più parti sulla base di effetti predefiniti dalle stesse” (art. 8 ter, secondo comma, del Decreto legge n. 135 del 2018 convertito con modifiche nella legge n. 12 del 2019)³⁵. Il linguaggio utilizzato dal legislatore che, per un verso, sembra prediligere la natura tecnico informatica dello *smart contract* stante la scelta di definirlo un programma per elaboratore che opera solo su “tecnologie basate su registri distribuiti” (art. 8 ter, primo comma)³⁶ e non su tecnologie diverse³⁷, e per altro, inserisce espliciti riferimenti al registro giuridico (esecuzione, vincola, parti, effetti), conferma proprio la sussistenza di due profili diversi ma strettamente connessi l’un l’altro.

Sulla base proprio del rapporto che lega codice informatico e accordo, gli *smart contracts*, perciò, possono essere semplici veicoli di scambio delle dichiarazioni negoziali; atti di esecuzione di contratti conclusi in forma tradizionale; o, ancora, fonti del vincolo negoziale “in quanto creano, modificano, trasferiscono diritti, doveri e poteri”³⁸.

In Australia si è ritenuto di applicare allo *smart contract* le previsioni dell’*Electronic Transactions Act*, 1999 (in <https://www.legislation.gov.au/Details/C2011C00445>) a norma del quale le transazioni elettroniche sono equiparate, quindi producono i medesimi effetti giuridici, a quelle analogiche. Il legislatore australiano ha esteso la previsione anche alle transazioni registrate su *blockchain*.

Gli Stati Uniti d’America ed altri Stati quali California, Delaware, Vermont, Nevada, Arizona, Hawaii, New Hampshire e Illinois, hanno introdotto una normativa volta a legittimare l’uso della tecnologia *blockchain* in generale, e dello *smart contract* in particolare. Le soluzioni sino ad ora adottate non sono però uniformi. Nel dettaglio, nello Stato del Vermont il legislatore ha previsto che un fatto, o un dato, verificato attraverso una valida applicazione della tecnologia *blockchain* è autentico e si considera certa la data e l’ora in cui la registrazione della transazione è avvenuta (<https://legislature.vermont.gov/bill/status/2016/H.868>). Parzialmente innovatore è stato invece il Governatore dello Stato dell’Arizona che introducendo una disciplina dedicata alle nuove tecnologie, ha equiparato la firma depositata su *blockchain* alla firma digitale (<https://legiscan.com/AZ/text/HB2417/id/1497439>). Anche il legislatore del Tennessee ha seguito un approccio analogo introducendo il 22 marzo 2018 due previsioni volte a legittimare le nuove tecnologie. In particolare, a norma della nuova versione del *Bill* n. 1662 i dati raccolti su *blockchain* hanno valore giuridico e uno *smart contract* può produrre effetti giuridici (<https://legiscan.com/TN/bill/SB1662/2017>). Decisamente più innovativa è invece la normativa californiana. La California Assembly ha varato la legge n. 2658 del 2018 che modifica il *California Civil Code*, assimilando lo *smart contract* ad un contratto tradizionale e chiarendo che il primo si distingue dal secondo solo per la forma (<https://legiscan.com/CA/text/AB2658/id/1732549>).

³⁴ Malta è stato il primo paese ad avere approvato una normativa in tema di regolazione della blockchain che ha lo scopo di promuoverne l’utilizzo sul territorio maltese al fine di incrementare gli investimenti e contribuire ad un miglioramento dell’economia nazionale (The Malta Digital Innovation Authority Act (MDIA Act), Innovative Technology Arrangements and Services Act (ITAS Act), e Virtual Financial Assets Act). Nel panorama europeo vanno segnalate, inoltre, le iniziative del governo lituano, che in collaborazione con la banca centrale nazionale ha lanciato il progetto di moneta virtuale LBCOINS basato sulla tecnologia blockchain e la recente definitiva approvazione, il 20 settembre 2020, da parte del Consiglio degli Stati della Svizzera, della “Legge federale sull’adeguamento del diritto federale agli sviluppi della tecnologia di registro distribuito” (sul punto N. TRAVIA, *Profili internazionali degli smart contract*, in AA.VV., *Blockchain e smart contract*, Milano, 2019, 394).

³⁵ D.l. n. 135 del 14 dicembre 2018, convertito in l. n. 12 dell’11 febbraio 2019, in *G.U.* n. 36 del 12 febbraio 2019 (Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione).

³⁶ All’art. 8 ter, primo comma, del d.l. n. 135/2018 così come convertito dalla l. n. 12/2019, è prescritto che si definiscono tecnologie basate su registri distribuiti “le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architettralmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l’aggiornamento e l’archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili”.

³⁷ L’esclusione, forse involontaria, del legislatore italiano è certamente contraria al principio della c.d. *neutralità tecnologica*, in base al quale il legislatore non deve interferire nello sviluppo di una specifica tecnologia per favorirla rispetto ad altre (E. CERVONE, *Strumenti di pagamento innovativi, interoperabilità e neutralità tecnologica: quali regole e quale governance per un mercato sicuro, efficiente ed innovativo*, in *Riv. trim. dir. econ.*, 2016, 61). Il principio, usato per la prima volta alla fine degli Anni 90 dall’Organizzazione Mondiale per il Commercio per l’accordo sulle telecomunicazioni, successivamente è stato utilizzato con riferimento specifico alla rete ed ai servizi di Internet. L’Unione Europea ha più volte fatto riferimento a tale principio per i servizi finanziari, l’intelligenza artificiale e, più in generale, per i nuovi sistemi digitali di pagamento (Corte di Giustizia, C-807/18 Telenor Magyarország & C-39/19 Telenor Magyarország, del 15/9/2020, in <http://curia.europa.eu>). Il principio è stato affermato a livello internazionale dalla Commissione delle Nazioni Unite per il Commercio internazionale (UNCITRAL) nel Model Law sugli Electronic Transferable Records approvato dalla Commissione il 13 luglio 2017.

³⁸ M. GIULIANO, *L’adempimento delle obbligazioni pecuniarie nell’era digitale*, Torino, 2018, 151.



Nei contratti stipulati a distanza (art. 1326), infatti, una parte può avvalersi di uno *smart contract* per trasmettere all'altra la proposta contrattuale³⁹. Lo *smart contract* assume in questo caso funzione “strumentale” ed ha, cioè, la stessa funzione che rivestirebbe una mail certificata. Solo che, a differenza della mail che viene trasmessa in un linguaggio “umano”, la proposta inviata tramite *smart contract*, prima di essere trasmessa, deve essere tradotta in un linguaggio informatico dal proponente (o da un tecnico abilitato) il quale, peraltro, dovrà premurarsi di precisare (a meno che non voglia concludere un contratto nella forma dello *smart contract*) che quella “versione” non ha alcun valore e non fa fede. L'oblato che si trova dinnanzi a una proposta trasmessagli tramite *smart contract* dovrà, a sua volta, prima decodificare il testo per comprendere il senso della proposta ricevuta e, di seguito, trasmettere l'accettazione mediante un altro *smart contract*. La farraginosità di questo meccanismo, ne rende piuttosto raro l'utilizzo come puro strumento di comunicazione.

Più frequentemente lo *smart contract* viene utilizzato per dare esecuzione ad un contratto tradizionale (funzione “esecutiva”)⁴⁰. Esso, cioè, diventa mezzo di adempimento delle obbligazioni “assunte prima ed altrove dalle parti” secondo le regole previste dal codice civile⁴¹. Ma non può ricorrersi allo *smart contract* per eseguire qualsiasi tipo contrattuale. Il suo utilizzo, infatti, è da escludere per i contratti che hanno esecuzione istantanea con contestuale esaurimento delle prestazioni reciproche salvo che residuino eventuali obbligazioni ulteriori, ad esempio di garanzia⁴²; parimenti non potrà farsi uso dello *smart contract* per eseguire prestazioni di fare o di consegnare beni materiali ovvero per realizzare effetti traslativi differiti, mentre ne sarà possibile l'utilizzazione per le prestazioni che abbiano ad oggetto il pagamento di somme di danaro o il trasferimento di beni dematerializzati⁴³. È dubbio se un contratto reale, per il quale la *traditio* è elemento della fattispecie, possa avere esecuzione a mezzo di uno *smart contract*. Se la consegna avviene al momento del perfezionarsi dell'accordo, la successiva esecuzione non presenta differenze rispetto ai contratti consensuali⁴⁴. Nel caso in cui lo *smart contract* sia utilizzato come mezzo di adempimento di obbligazioni contrattuali

³⁹ R. SACCO, G. DE NOVA, *Il contratto*, Torino, 2016, 125 ss.

⁴⁰ N. SZABO, *Smart Contracts: Building Blocks for Digital Markets*, cit., secondo cui l'esecuzione di un contratto rappresenta l'alveo naturale di utilizzo dello *smart contract*. Szabo, infatti, descrive un *smart contract* assimilandolo ad una *vending machine*, ovvero ad un comune distributore automatico. Per il famoso criptografo, uno *smart contract* altro non è che la trasposizione in termini digitali di un treno di ingranaggi; con la grande differenza che mentre un meccanismo, per quanto sofisticato, sarà sempre piuttosto rigido nella propria esecuzione, uno *smart contract* è estremamente flessibile. Mentre infatti una macchina distributrice, richiede una moneta di un determinato taglio e rilascia un solo chewing-gum tra quelli contenuti nella tramoggia, uno *smart contract*, su piattaforma che ospita un linguaggio Turing-completo, consente una varietà pressoché infinita di input, in ingresso e in uscita. Uno *smart contract*, quindi, eleva la complessità dell'interazione ai massimi livelli. È questa l'intuizione di Szabo: la costruzione di una *vending machine universale* capace cioè di eseguire un numero indeterminato di compiti.

⁴¹ F. RAMPONE, *Smart contract: né smart né contract*, in *Riv. dir. priv.*, 2019, 2, 8.

⁴² Si pensi, ad esempio, all'ipotesi in cui in una operazione di compravendita di partecipazioni societarie, si preveda la stipulazione di uno *share purchase agreement* che regoli i rapporti tra acquirente e venditore nel caso di sopravvenienze di passività che possano emergere nel periodo di tempo intercorrente tra la firma (*signing*) e il passaggio di proprietà (*closing*) o addirittura nella fase successiva (*post closing*). Lo *share purchase agreement*, essendo un contratto del tutto autonomo rispetto a quello di compravendita, ben può essere stipulato facendosi ricorso ad uno *smart contract* (A. MASTRANGELO, *The sale and purchase agreement (spa)*, in <https://www.diritto.it>).

⁴³ D. AQUARO, *Smart contract: cosa sono (e come funzionano) le clausole su blockchain*, in <https://www.ilsole24ore.com>.

⁴⁴ S. CERRATO, *Contratti tradizionali, diritto dei contratti e smart contract*, in AA.VV., *Blockchain e smart contract*, Milano, 2019, 291. In effetti una tale ricostruzione giuridica del fenomeno potrebbe in verità comportare dei problemi applicativi qualora, ad esempio, due parti decidano di regolare tra loro un determinato rapporto prevedendo, per la fase esecutiva, la redazione di uno *smart contract* che, a determinate scadenze, provveda a trasferire una criptovaluta quale corrispettivo di una prestazione, magari da svolgere “off-chain”. L'oblato di detta prestazione, confidente dello *smart contract*, esegue la prestazione, mentre la parte debitrice dell'obbligazione di pagamento, per sfuggire alla stessa, non provvede al deposito sull'indirizzo dello *smart contract* della criptovaluta



già definite in un contratto tradizionale sorge anche qui, innanzitutto, il problema di tradurre il testo in linguaggio informatico. La traduzione del contratto concluso in modo tradizionale costituisce in questa peculiare ipotesi una sorta di ripetizione del contratto “in una forma diversa e necessaria per la sua esecuzione”⁴⁵. Se la ripetizione del contratto ad opera del “traduttore” avviene in maniera corretta *nulla quaestio*, ma se il contenuto dello *smart contract* è diverso da quello che le parti avevano concluso, vista la sua stabilità ed irrettrattabilità, esso potrà essere reso inefficace solo con un intervento successivo dell’operatore ed il redattore dello *smart contract* sarà ritenuto responsabile e dovrà risarcire i danni subiti dalle parti⁴⁶. In sede di ripetizione dello *smart contract* non è da sottovalutare la funzione “*if ... then ...*”, tipica di questa fattispecie, la quale prevede che, al verificarsi di determinati presupposti (*if ...*) previsti dal programmatore e che sono accertabili attraverso gli *imput* provenienti dai c.d. “oracoli”⁴⁷, lo *smart contract* si avvia e dà luogo all’esecuzione del contratto (... *then*)⁴⁸. La funzione “*if ... then ...*” può qualificarsi giuridicamente come condizione (art. 1353 ss. cod. civ.) o termine qualora le parti nell’accordo negoziale abbiano previsto un evento futuro e incerto o una data cui subordinare l’efficacia del contratto. Viceversa, nell’ipotesi in cui il contratto sia già pienamente efficace, la funzione “*if ... then ...*” funge soltanto da presupposto per l’adempimento dell’altrui prestazione. Le parti cioè, possono istruire il *software* perché esegua la prestazione solo previa conferma, data tramite un “*oracolo*”, dell’altrui adempimento⁴⁹. Sia nell’una che nell’altra circostanza, comunque, l’esecuzione automatica della struttura *if ... then ...* è la caratteristica idonea a rendere lo *smart contract* preferibile rispetto agli strumenti tradizionali in quanto darebbe alle parti la certezza che la

corrispondente. In questo caso il contratto non potrebbe dirsi eseguito in quanto non viene attuato alcun trasferimento e secondo la norma non sarebbe suscettibile di tutela, proprio perché ancora non perfezionato (M. NICOTRA, *L’Italia prova a normare gli smart contract, ecco come: pro e contro*, in <https://www.agendadigitale.eu>).

⁴⁵ Di V. GRAVIO, *Dichiarazione riproduttiva*, in *Dig. it. disc. priv.*, sez. civ., Torino, 1989, V. 366; A. GENTILI, *La replica della stipula: riproduzione, rinnovazione, rinegoziazione del contratto*, in *Contratto impr.*, 2003, 667.

⁴⁶ S. CAPACCIOLI, *Smart contracts: traiettoria di un’utopia divenuta attuabile*, Modena, 2016, 42.

⁴⁷ Con il termine “oracolo” si intende far riferimento ad un “sensore esterno” cui è attribuito il compito di certificare l’avverarsi delle condizioni poste alla base del regolamento contrattuale, andando a costituire l’input di attivazione delle prestazioni automatizzate previste secondo i criteri in questa sede analizzati. L’oracolo può essere basato su un *software*, su un *hardware* o su intermedio umano. Gli oracoli *software* estraggono le informazioni necessarie on line o in altre blockchain e le inseriscono nel contratto intelligente. Negli oracoli *software* la questione principale è data dalla fonte da cui l’informazione è tratta che può essere una fonte sicura e affidabile (ad esempio nel caso di Wikipedia) o incerta. In quest’ultimo caso l’oracolo rende errato il dato prelevato. Gli oracoli *hardware* offrono un modo sicuro e non manomissibile per raccogliere i dati dai sensori degli oggetti collegati (si pensi ai sensori collegati ad una automobile che sono capaci di rilevarne la velocità di marcia). Per potere segnalare in modo sicuro una lettura da un sensore, gli oracoli *hardware* richiedono una attestazione crittografica della lettura del sensore, al fine di autenticare l’origine della misurazione, nonché una installazione anti-manomissione del dispositivo lettore che offra la misura di sicurezza di rendere inutilizzabile l’oracolo in caso di tentativo di manomissione. Gli oracoli umani sono necessari per la convalida di richieste complesse. Ad esempio, un operatore umano è in grado di discernere il grado e l’entità di un danno fisico, a seguito di una visita medica, e di indicarlo nella relativa voce all’interno di un contratto di assicurazione (E. BATTELLI, *Le nuove frontiere dell’automatizzazione contrattuale tra codici algoritmici e big data: gli smart contracts in ambito assicurativo, bancario e finanziario*, in *Giust. civ.*, 2020, 4, 681). A parte queste che sono le tipologie più note di oracoli, ne esistono delle altre. Si pensi agli oracoli basati sul consenso (ad esempio *Augur* o *Gnosis*) che si caratterizzano per il fatto che ai fini della risoluzione di un problema o della decisione di un evento ci si basa “sulla saggezza della folla” cioè sul parere di più oracoli contemporaneamente. Non sono, da ultimo, da trascurare la possibilità di una rete di oracoli distribuiti basati su token, gli oracoli inbound e gli oracoli outbound (M.T. GIORDANO, *Il problema degli oracoli*, in AA.VV., *Blockchain e smart contract*, cit., 260).

⁴⁸ P. CUCCURU, *Beyond bitcoin: an early overview on smart contracts*, in *International Journal of Law and Information Technology*, XXV, 2017, 179 ss.

⁴⁹ “Ciò che le parti intendono perseguire ricorrendo allo *smart contract* è la certezza dell’adempimento reciproco, un obiettivo a cui il nostro ordinamento preordina alcuni strumenti attivabili per volontà negoziale (ad esempio prevedere una garanzia escutibile anche a prima richiesta) o in autotutela come nel caso dell’eccezione di inadempimento ex articolo 1460 cod. civ.” (S. CERRATO, *Contratti tradizionali, diritto dei contratti e smart contract*, cit., 293).



prestazione dedotta in contratto si eseguirà nel modo prescritto nel *software*, “senza richiedere l’intervento di un terzo, quale è il giudice, il cui intervento diverrebbe superfluo”⁵⁰.

Il testo del contratto tradotto in linguaggio informatico, da ultimo, dovrà essere sottoscritto dalle parti e dovranno essere sottoscritte, se presenti, le eventuali clausole vessatorie⁵¹. Il meccanismo di sottoscrizione più diffuso è quello della crittografia asimmetrica o a doppia chiave che consente di poter imputare univocamente una transazione ad un soggetto⁵². È da sottolineare, però, che la mancata identificazione informatica delle parti di uno *smart contract* con solo fini esecutivi non rende invalido l’atto, che resta subordinato “alle dinamiche negoziali del mondo reale. Dunque, potranno al più porsi dubbi circa l’identità del soggetto attivo o passivo dell’intervenuto adempimento e le conseguenti eventuali azioni di indebito, per esempio nel caso in cui il creditore lamenti di non aver ricevuto la prestazione e il debitore affermi che essa è stata regolarmente eseguita dallo *smart contract*, salvo poi acquisire consapevolezza del fatto che essa sia stata rivolta a beneficio di un terzo erroneamente identificato come il creditore all’interno dello *smart contract*”⁵³.

4. – Non vi sono ostacoli a considerare lo *smart contract* come veicolo atto a dar luogo alla redazione di un contratto⁵⁴. Nel nostro ordinamento, infatti, vige il principio della libertà della forma del contratto, ragion per cui la manifestazione del programma negoziale può avvenire con dichiarazione orale, con comportamento concludente, con dichiarazione per iscritto o, appunto, per via informatica⁵⁵. Con riferimento alla particolare modalità di manifestazione del consenso negli *smart contracts*, e in genere nei contratti telematici o ciberneticici, pur nella loro differente struttura, il legislatore nazionale dapprima con l. n. 59 del 15 marzo 1997⁵⁶ e con il d.P.R. n. 513 del 10 novembre 1997⁵⁷, poi trasfuso nel d.P.R. n. 445 del 28 dicembre 2000⁵⁸,

⁵⁰ B. CAPIELLO, *Dallo “smart contract” computer code allo smart (legal) contract. I nuovi strumenti (para) giuridici alla luce della normativa nazionale e del diritto internazionale privato europeo: prospettive de jure condendo*, in *Dir. comm. int.*, 2020, 477.

⁵¹ Per la sottoscrizione delle clausole vessatorie i tecnici suggeriscono due possibilità. La prima si fonda sull’inserire nello *smart contract* di una condizione sospensiva consistente nella sottoscrizione – che avverrebbe nel mondo reale – delle clausole vessatorie, il cui avveramento sarebbe comunicato tramite oracolo allo *smart contract*. La seconda, che avrebbe il pregio di risolvere l’intera questione in rete, ipotizza di scindere l’unitario *smart contract* in due, che la parte dovrebbe sottoscrivere in sequenza: il primo di essi contenente soltanto le clausole vessatorie che richiedono la doppia sottoscrizione e il secondo, che si attiverebbe solo una volta sottoscritto il primo, contenente tutte le clausole del regolamento contrattuale (F. BENATTI, *Un nuovo paradigma contrattuale: el caso de los smart contracts*, in AA.VV., *Derecho y nuevas tecnologías. El impacto de una nueva era*, Lima, 2019, 275 ss.). Non è, invece, per nulla conforme alla doppia sottoscrizione l’approvazione delle clausole vessatorie con il c.d. “point and click” (Giudice di pace di Milano, sentenza del 28 gennaio 2019, in *Banca dati pluris*; Tribunale di Catanzaro, sentenza del 30 aprile 2012, in *Contratti*, 2013, 41).

⁵² Il sistema di crittografia asimmetrica o a doppia chiave, come si deduce dal nome, attribuisce ad ogni attore coinvolto nella comunicazione una coppia di chiavi: la chiave pubblica, che deve essere distribuita e la chiave privata, appunto personale e segreta. Si evita così qualunque problema connesso alla necessità di uno scambio in modo sicuro dell’unica chiave utile alla cifratura/decifratura presente invece nella crittografia simmetrica. Il meccanismo si basa sul fatto che, se con una delle due chiavi si cifra (o codifica) un messaggio, allora quest’ultimo sarà decifrato solo con l’altra.

⁵³ S. CERRATO, *Appunti su smart contract e diritto dei contratti*, in *Banca, borsa, tit. cred.*, 2020, 3, 370 ss.

⁵⁴ Sul sito <https://www.cryptominando.it/> 2018 può trovarsi tutto il procedimento per creare uno *smart contract*. In dottrina si veda R. BATTAGLINI, P. NICORELLI, *Smart legal contract. Dall’idea al codice*, Milano, 2021.

⁵⁵ F. CARNELUTTI, voce *Documento* (Teoria moderna), in *Noviss. dig. it.*, Torino, 1964, IV, 86, evidenziava l’irrelevanza della materia, affermando che “qualunque materia, atta a formare una cosa rappresentativa, può entrare nel documento: tela, cera, metallo, pietra e via dicendo”.

⁵⁶ L. n. 59 del 15 marzo 1997 (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 amministrativa), in *G.U.* n. 63 del 17 marzo 1997.

⁵⁷ D.P.R. n. 513 del 10 novembre 1997 (Regolamento recante criteri e modalità per la formazione, l’archiviazione e la trasmissione



e poi con il CAD⁵⁹, ha affermato il principio della piena validità dei contratti stipulati per via informatica o telematica, prevedendo che “gli atti, dati e documenti formati dalla pubblica amministrazione 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”. Attraverso uno *smart contract*, dunque, le parti possono esprimere una dichiarazione intesa a realizzare un contenuto giuridicamente vincolante, imputabile direttamente ai soggetti ai quali i codici digitali sono legati e che si attua secondo quanto programmato⁶⁰. Può ipotizzarsi che alla stesura di uno *smart contract* si pervenga a seguito di trattative condotte tra le parti (art. 1337 cod. civ.) ovvero dopo che sia stato stilato un contratto preliminare (art. 1351 cod. civ.) che prelude alla redazione di un definitivo sotto forma di *smart contract*. Nulla osta alla configurabilità di una opzione di *smart contract* (art. 1331 cod. civ.), ovvero alla possibilità di una proposta strutturata sotto forma di proposta irrevocabile (art. 1329 cod. civ.). Poiché il secondo comma dell’art. 8 ter del D.L. 135/2018 precisa che lo *smart contract* deve “vincolare automaticamente due o più parti” risultano esclusi dalla normativa “tutti quegli applicativi su DLT che non hanno effetto su almeno due parti quali gli *smart contract* di natura meramente procedurale, di emissione di token⁶¹ o di attestazione di informazioni o eventi”⁶². Peraltro, poiché la norma aggiunge che il vincolo automatico creato dallo *smart contract* sulle parti deve essere basato su “effetti predefiniti dalle stesse”, vanno altresì esclusi dall’applicazione della norma in commento gli *smart contract* sviluppati da una sola parte o che implicino un meccanismo di semplice accettazione per adesione dell’altra parte (ad esempio gli *smart contract* che prevedano una offerta al pubblico o un contratto aperto)⁶³.

Poiché lo *smart contract* va redatto con un linguaggio informatico, comprensibile agli algoritmi operanti nel protocollo⁶⁴, non è strutturato per messaggi complessi e può contenere solo l’indicazione delle parti, la determinazione o determinabilità dell’oggetto e la causa (art. 1325 cod. civ.). Lo *smart contract*, dunque, ha uno scheletro minimo sufficiente che non ammette formule ambigue o dal significato oscuro⁶⁵. È improponibile che esso possa prevedere, come avviene in un contratto tradizionale, dichiarazioni di scienza, defini-

ne di documenti con strumenti informatici e telematici, a norma dell’articolo 15, comma 2, della legge 15 marzo 1997, n. 59), in *G.U.* n.60 del 13 marzo 1998.

⁵⁸ d.P.R. n. 445 del 28 dicembre 2000 (Disposizioni legislative in materia di documentazione amministrativa), in *G.U.* n. 42 del 20 febbraio 2001.

⁵⁹ Il Codice dell’Amministrazione Digitale (CAD) è un testo unico che riunisce e organizza le norme riguardanti l’informatizzazione della Pubblica Amministrazione nei rapporti con i cittadini e le imprese. Istituito con il d.lgs. n. 82 del 7 marzo 2005, è stato successivamente modificato e integrato prima con il d.lgs. n. 179 del 22 agosto 2016 e poi con il d.lgs. n. 217 del 13 dicembre 2017 per promuovere e rendere effettivi i diritti di cittadinanza digitale.

⁶⁰ M. GIULIANO, *L’adempimento delle obbligazioni pecuniarie nell’era digitale*, cit., 170.

⁶¹ Un *token* è un insieme di informazioni digitali all’interno di una blockchain che conferiscono un diritto a un determinato soggetto. La *tokenizzazione* è la conversione dei diritti di un bene in un token digitale registrato su una blockchain.

⁶² R. BATTAGLINI, *La normativa italiana sugli smart contract*, in AA.VV., *Blockchain e smart contract*, Milano, 2019, 379.

⁶³ M. NICOTRA, *L’Italia prova a normare gli smart contract, ecco come: pro e contro*, cit., *Contra* G. GUIDA, *Blockchain e smart contract: benefici e limiti*, in <https://www.altalex.com> e A. CONTALDO, F. CAMPARA, *Blockchain criptovalute, smart contract, industria 4.0*, Pisa 2019, 59 secondo cui lo *smart contract* è in grado di stabilire, parimenti all’offerta al pubblico dove una parte è vincolata alle proprie dichiarazioni in qualità di proposta a contrarre, degli obblighi solo nei confronti di una parte la quale, da un lato, si occuperà della formalizzazione dei medesimi all’interno di uno *smart contract* e, dall’altro, darà esecuzione alle prestazioni al verificarsi di certe condizioni.

⁶⁴ E. MIK, *Smart contract: terminology, technical limitations and real world complexity*, in *Law, innovation and technology*, 2017, 9.

⁶⁵ M. RASKIN, *The law and legality of smart contract*, in *Georgetown law technology review* 2017, 325 afferma che “ambiguity is anathema to computer language”.



zioni, clausole d'uso, premesse, allegati etc.; né che allo *smart contract* venga allegata scrittura *inter partes* integrativa, formulata in linguaggio naturale che disciplini determinate variabili e rinvii eventuali controversie avanti il giudice naturale o una corte arbitrale (c.d. *smart contract ibrido*)⁶⁶.

Il linguaggio crittografico deve essere espresso in maniera chiara e le parti devono essere in grado di intendere il contenuto del testo. L'intelligibilità è elemento caratterizzante e fondamentale ai fini della validità dello *smart contract*. Il che, però, non significa che esso possa regolare solo i rapporti B2B o B2b, in cui le parti contraenti (o almeno una di esse) dispongano del potere contrattuale ed economico e – soprattutto – della capacità tecnica e professionale necessari a elaborare tali contratti in formato crittografico⁶⁷. Nulla toglie, infatti, che lo *smart contract*, operante su tecnologia DLT⁶⁸, possa essere utilizzato anche da privati. L'importante è che essi diano prova di comprendere il significato dello *smart contract*, il che può avvenire “sia per espressa loro ammissione effettuata in linguaggio naturale, sia per deduzione in considerazione delle loro comprovate competenze tecniche”. In entrambi i casi si tratta di accertare se le parti sono “in grado di

⁶⁶ Si tratta, infatti, di un'integrazione che priva lo *smart contract* del suo carattere automatico e incorruttibile. Lo *smart contract* rimarrebbe per questo solo l'elemento di prova di un accordo originario tra le parti, poi disciplinato in modo tradizionale, ossia attraverso la predisposizione della citata scrittura integrativa. Tale eventualità incrementa la tutela delle parti ma “snatura” lo strumento giuridico, considerato che rende la sua auto esecutività “relativa” e non esclusiva, essendo esposta alla volontà della parte presunta lesa di iniziare un procedimento giudiziario. Da quanto precede, si può concludere che uno *smart contract ibrido* può essere qualificabile come contratto in senso tradizionale solo se non poggia sull'esclusiva esecuzione informatica (F. CARBONE, *Cos'è Chainlink (LINK), e futuro degli smart contract ibridi*, in <https://www.fxempire.it/e>).

⁶⁷ In particolar modo si pensi a settori quali quello bancario, finanziario ed assicurativo tra i primi ad aver recepito le opportunità che le nuove tecnologie (E. BATTELLI, *Le nuove frontiere dell'automatizzazione contrattuale tra codici algoritmici e big data: gli smart contracts in ambito assicurativo, bancario e finanziario*, in *Giust. civ.*, 2020, 681). Nel settore bancario gli *smart contract* rappresentano lo strumento informatico capace di realizzare i c.d. *instant payment* cioè i trasferimenti di denaro immediati che sfruttano la disintermediazione della catena di blocchi su cui sono codificati (A. CALONI, *Deposito di criptoattività presso una piattaforma exchange: disciplina e attività riservate*, in *Giur. comm.*, 2020, 5, 1073; E. BATTELLI, E. INCUTTIM., *Gli smart contract nel diritto bancario tra esigenze di tutela e innovativi profili di applicazione*, in *Contr. impr.*, 2019, 925; S.L. FURNARI, *Validità e caratteristiche degli smart contracts e possibili usi nel settore bancario finanziario*, in AA.VV., *I diversi settori del Fintech*, Padova, 2019, 106; R. GARAVAGLIA, *Finalità, funzionamento e tipologia di utilizzi delle Blockchain*, in *Quaderni di ricerca giuridica della Banca d'Italia*, 2019, 177); in quello finanziario esso si adatta al trasferimento delle c.d. *stock options* che attribuiscono la facoltà di acquistare azioni o titoli rappresentativi del capitale di rischio della società, entro un determinato periodo di tempo e ad un dato prezzo (M.T. PARACAMPO, *La consulenza finanziaria automatizzata*, in AA.VV., *Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, Torino, 2017, 127; AA.VV., *Valore della consulenza finanziaria e robo advice nella percezione degli investitori. Evidenze da un'analisi qualitativa*, in *Quaderni Fintech Consob*, Milano, 2019, 6; R. LENER, *La «digitalizzazione» della consulenza finanziaria. Appunti sul c.d. robo-advice*, in *Quaderni di Minerva Bancaria*, 2018, 2). Nel settore assicurativo è prospettabile l'utilizzo di uno *smart contract* posto alla base di una determinata copertura assicurativa contro i danni causati dalla circolazione del proprio veicolo che si attiverebbe automaticamente al realizzarsi del sinistro stradale attraverso i sensori inseriti al suo interno. Ovvero un'altra ipotesi applicativa molto interessante è quella adoperata da alcune compagnie di assicurazione in relazione a contratti assicurativi che coprono il costo dei biglietti aerei a causa di ritardi o cancellazione del volo. In queste ipotesi, lo *smart contract*, una volta verificatosi l'evento (ritardo o cancellazione del volo), opera in automatico il rimborso previsto in sede contrattuale connettendo il conto corrente del consumatore-assicurato con quello dell'impresa (E. BATTELLI, *Big data e algoritmi predittivi nel settore assicurativo: vantaggi e nuovi rischi*, in *Corr. giur.*, 2019, 1517; G. D'IPPOLITO, E. INCUTTIM., *I processi decisionali interamente automatizzati nel settore assicurativo*, in *Media laws*, 2019, 2, 745).

⁶⁸ Va osservato che la formulazione del secondo comma dell'art. 8-ter l. n. 12/2019 risente di un errore di sovrapposizione tra le tecnologie basate su registro distribuito (DLT) di cui al primo comma dello stesso articolo e blockchain con il risultato che il legislatore considera *smart contract* solo quello operante su DLT. Da ciò, ovviamente, la esclusione di tecnologie diverse. Tale esclusione contravviene al principio di “neutralità tecnologica” in base al quale il legislatore non deve interferire nello sviluppo di una specifica tecnologia per favorirla rispetto ad altre. Tale principio, affermato a livello internazionale dalla Commissione delle Nazioni Unite per il Commercio internazionale (UNCITRAL) è stato ribadito in sede comunitaria (E. CERVONE, *Strumenti di pagamento innovativi, interoperabilità e neutralità tecnologica: quali regole e quale governance per un mercato sicuro, efficiente ed innovativo*, in *Riv. trim. dir. econ.*, 2016, 61).



avere accesso e di comprendere il significato del codice di programmazione con cui è predisposto lo *smart contract* e le conseguenze della sua esecuzione, attribuendo quindi ad esso la fonte primaria delle loro obbligazioni”⁶⁹. Nel caso in cui il linguaggio informatico non sia compreso pienamente, parte della dottrina ritiene plausibile che le parti possano accompagnare lo *smart contract* con una versione del contratto espressa con un linguaggio naturale⁷⁰.

5. – Qualora lo *smart contract* sia fonte del vincolo negoziale (abbia cioè “funzione costitutiva”), esso non può essere utilizzato per stipulare un contratto che richieda la forma solenne (atto pubblico o scrittura privata autenticata). Piuttosto ai sensi del comma 2 dell’art. 8-ter del d.l. n. 235/2018, esso soddisfa “il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall’Agenzia per l’Italia digitale con linee guida da adottare entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto”. Ciò significa che la sottoscrizione digitale dello *smart contract* sulla blockchain, ove avvenga secondo i dettami fissati nelle linee guida predisposte dal Ministro per l’innovazione tecnologica (MITD)⁷¹, dota lo *smart contract* del requisito della “forma scritta” (artt. 20 e 21 del Codice dell’Amministrazione Digitale)⁷². In particolare lo *smart contract* può soddisfare il requisito della forma scritta ed ha l’efficacia prevista nell’art. 2702 cod. civ. quando vi sia apposta “una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall’AgID ai sensi dell’art. 7” (art. 20 CAD). Le parti della transazione devono, dunque, essere identificate⁷³. Ma, a differenza di quando accade per l’identificazione dei soggetti in moduli o documenti cartacei cui deve provvedere la pubblica autorità⁷⁴, per i documenti informatici l’effetto di cui all’art. 2702 cod. civ. si consegue attraverso l’apposizione di una firma elettronica avanzata⁷⁵ o qualificata⁷⁶ o attraverso l’identificazione

⁶⁹ RAMPONE, *Smart contract: né smart né contract*, cit., 10.

⁷⁰ A. STAZI, *Automazione contrattuale e contratti “intelligenti”. Gli smart contract nel diritto comparato*, Torino, 2019, 147.

⁷¹ Il Ministro per l’innovazione tecnologica e la transizione digitale (MITD) ha emanato le suddette Linee guida per l’implementazione di SPID/CIE, PAGOPA e app IO che sono entrate in vigore il 28 febbraio 2021, in <https://innovazione.gov.it>.

⁷² Il Codice dell’Amministrazione Digitale (CAD) è un testo unico che riunisce e organizza le norme riguardanti l’informatizzazione della Pubblica Amministrazione nei rapporti con i cittadini e le imprese. Istituito con il d.lgs. 7 marzo 2005, n. 82, è stato successivamente modificato e integrato prima con il d.lgs. 22 agosto 2016 n. 179 e poi con il d.lgs. 13 dicembre 2017 n. 217 per promuovere e rendere effettivi i diritti di cittadinanza digitale.

⁷³ Per la risoluzione del problema attinente l’identificazione *on line* era già stata determinante l’emanazione del Regolamento (UE) n. 910 del 23 luglio 2014 (in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva CE n. 93 del 1999), in *G.U.U.E.* L 257/73 de 28 agosto 2014. Il regolamento è comunemente denominato “EIDAS”, dove “e” sta per “electronic”, “ID” per “identification”, “A” per “authentication” e “S” per “signature”. Oggetto del regolamento, infatti, oltre all’identificazione *on line* sono anche le firme elettroniche e i cosiddetti servizi fiduciari o trust service. Il regolamento distingue fra identificazione elettronica e autenticazione elettronica. L’identificazione elettronica (electronic identification) è il procedimento di utilizzo dei dati personali identificativi in forma elettronica al fine di rappresentare in modo univoco una persona fisica o giuridica, o la persona fisica che rappresenta una persona giuridica (articolo 3, n. 1, Regolamento EIDAS); mentre l’autenticazione (authentication) è definita come il processo elettronico che consente di confermare l’identificazione elettronica di una persona fisica o giuridica, o l’origine e l’integrità dei dati in forma elettronica (Articolo 3, n. 5, Regolamento e-IDAS). Sul punto per tutti F. DELFINI, *Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, commento al regolamento UE 910/2014*, Torino, 2017.

⁷⁴ Si vedano in tal senso l’art. 51 della l. n. 89 del 16 febbraio 1913 (Codice della legge notarile); gli artt. 18, 21, 30, 31 e 45 del d.P.R. n. 445 del 28 dicembre 2000 (Disposizioni legislative in materia di documentazione amministrativa); e l’articolo 163 c.p.c.

⁷⁵ La firma elettronica avanzata (FEA) è un particolare tipo di firma elettronica con il quale si possono firmare tutti gli atti ad esclusione dei contratti relativi a beni immobili (per i quali è richiesta l’apposizione della firma digitale).



con firma digitale secondo i criteri fissati dall’Agenzia per l’Italia digitale (con SPID, CIE etc.). In particolare ai sensi dell’art. 21 CAD “le scritture private di cui all’articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale. Gli atti di cui all’articolo 1350, numero 13 del codice civile redatti su documento informatico o formati attraverso procedimenti informatici sono sottoscritti, a pena di nullità, con firma elettronica avanzata, qualificata o digitale ovvero sono formati con le ulteriori modalità di cui all’articolo 20, comma 1-bis, primo periodo”. In tutti i casi in cui la sottoscrizione non avvenga secondo i dettami normativi previsti “l’idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità” (art. 20 CAD).

La sottoscrizione del documento, compiuta dalle parti (o da loro rappresentanti)⁷⁷, certifica il consenso prestato dalle stesse imputando loro le decisioni assunte⁷⁸, fornisce validità giuridica alle transazioni concluse in ambiente virtuale rendendole immutabili⁷⁹, e, infine, garantisce la sicurezza di tutti i consociati⁸⁰. È pur vero, però, che esiste sempre un margine di incertezza dettato dal fatto che colui il quale utilizza la firma in un dato momento non sia anche il titolare della stessa ma che se ne sia appropriato illecitamente⁸¹. Sul punto

⁷⁶ La firma elettronica qualificata (FEQ) – o digitale – è il risultato di una procedura informatica, detta validazione, che garantisce l’autenticità, l’integrità e il non ripudio dei documenti informatici.

⁷⁷ È ammissibile la sottoscrizione dello *smart contract* per procura fermo restando, però, che il conferimento ad un terzo del potere di spendere il proprio nome resterà saldamente ancorato al mondo reale non essendo configurabile una procura in formato *smart*. Il procuratore, sulla base dei poteri conferitigli, potrà negoziare e sottoscrivere lo *smart contract*. Occorrerà, però, che il rappresentato ponga in essere alcune attività ulteriori che devono essere verificate di volta in volta (ad esempio messa a disposizione delle criptovalute per eseguire la transazione).

⁷⁸ Pur volendo prendere atto dell’autonoma capacità elaborativa della blockchain o dei registri distribuiti non si può giungere infatti ad una soggettivazione del codice informatico che rappresenta solo lo strumento di manifestazione di una volontà in altro modo formatasi (R. BORRUSO, *Computer e diritto*, Milano, 1998, 350).

⁷⁹ Il contenuto dei blocchi sulla catena impedisce che lo *smart contract* possa essere modificato o sciolto. L’istituto del mutuo dissenso di cui all’articolo 1372 cod. civ. non è nella fattispecie *de qua* assolutamente prospettabile. Le parti per neutralizzare gli effetti giuridici patrimoniali prodotti dallo *smart contract* possono predisporre un nuovo *smart contract* di contenuto uguale e contrario ovvero possono prevedere un *kill code* attivabile indifferentemente da una qualunque delle parti. Non diversa è la soluzione per l’esercizio del diritto di recesso unilaterale (art. 1373 cod. civ.), seppure la Risoluzione del Parlamento Europeo del 20 ottobre 2020 inviti espressamente gli Stati membri “a prevedere misure atte ad assicurare che i contratti intelligenti siano dotati di meccanismi in grado di arrestarne o di invertirne l’esecuzione”. Dunque l’obbligo per gli Stati esiste ma è un obbligo distonico con il meccanismo ed il funzionamento dello *smart contract*. Astrattamente, si potrebbe prevedere di dotare lo *smart contract* di un oracolo esterno che accerti la volontà di recedere del consumatore e che, di seguito, invii l’input di retrocessione. Si tratterebbe, però, di un rimedio non gratuito e non in linea con le esigenze di certezza dell’esecuzione cui rispondono gli *smart contract*.

⁸⁰ La certezza circa le parti di un qualsiasi rapporto giuridico rientra tra i principi sicuramente di ordine pubblico interno ma anche internazionale ove i contratti si concludano tra soggetti residenti in stati diversi. Sul rapporto tra ordine pubblico interno ed internazionale, a solo titolo esemplificativo, si vedano: G. PERLINGIERI, G. ZARRA, *Ordine pubblico interno e internazionale tra caso concreto e sistema ordinamentale*, Napoli, 2019; F. MOSCONI, C. CAMPIGLIO, *Diritto internazionale privato e processuale*, Milano, 2017, 256-273; O. FERACI, *L’ordine pubblico nel diritto dell’unione europea*, Milano, 2012; N. BOSCHIERO, *Ordine pubblico “internazionale” e norme di applicazione necessaria*, in AA.VV., *Atti notarili, diritto comunitario e internazionale*, Torino, 2011, I, 137; L. FUMAGALLI, *L’ordine pubblico nel sistema del diritto internazionale privato comunitario*, in AA.VV., *Il diritto del commercio internazionale*, Padova, 2004, 635 ss.; F. MOSCONI, *Il limite dell’ordine pubblico nella Convenzione di Bruxelles del 1968 sulla competenza giurisdizionale e l’esecuzione delle decisioni in materia civile e commerciale*, in *Jus* 1990.

⁸¹ Una certezza in tal senso si può avere solo con l’utilizzo di firme grafometriche o biometriche, magari combinate con le altre firme elettroniche o certificazioni. La firma grafometrica o biometrica è una firma elettronica particolare. Al firmatario viene richiesto di apporre una firma per mezzo di una penna elettronica su una sorta di tablet (o pad di firma); la piattaforma è progettata appositamente per individuare le caratteristiche dinamiche della firma. I dati raccolti dal dispositivo sono molteplici, e comprendono la pressione esercitata, il tratto e la velocità di firma. Tali informazioni vanno a “fondersi” in modo permanente con il documento sottoscritto, permettendo agli stessi dati di non poter essere modificati. Tali elementi, una volta acquisiti da banche, assicurazioni, società



una sentenza del Tribunale di Roma, depositata il 23 gennaio 2017, mette proprio in evidenza l'aspetto debole della firma digitale che certamente non assicura che sia stato proprio il titolare ad utilizzare e ad autorizzare la transazione o sottoscrivere un atto⁸². Il Tribunale ha ritenuto che in relazione al tipo di documento (informatico) e di firma (digitale) l'uso del dispositivo si presume riconducibile al titolare salvo che questi, ai sensi del disposto di cui all'art. 21, comma 2, del Codice sull'amministrazione digitale (CAD), non fornisca la prova contraria. Si realizza, pertanto, un'inversione dell'onere della prova in quanto compete a chi opera il disconoscimento della sottoscrizione smentire di averla effettuata provando di non aver apposto la firma digitale⁸³. Con la conseguenza implicita che, provando di non avere inserito la propria firma (codice identificativo), il soggetto dimostra di non avere espresso alcun consenso e, quindi, di non essersi voluto vincolare.

6. – Nella tecnologia blockchain la crittografia e l'utilizzo di firme elettroniche sono tecniche di pseudonimizzazione⁸⁴. Esse, cioè consentono di individuare l'indirizzo informatico delle parti ma non la loro identità. I dati personali, ai sensi dell'art. 4 del Regolamento CE n. 679 del 2016 (GDPR)⁸⁵, possono essere attribuiti ad un soggetto specifico solo con l'utilizzo di informazioni aggiuntive che, però, devono essere conser-

di servizi, studi professionali, possono essere utilizzati per identificare il firmatario. È stata l'Autorità Garante per la protezione dei dati personali, mediante un provvedimento datato 31 gennaio 2014, a seguito di una Verifica preliminare richiesta da IT Telecom s.r.l. e Cassa di Risparmio di Parma e Piacenza, ha rilevato che "il trattamento dei dati biometrici che le società istanti intendono effettuare, in base alla documentazione prodotta e alle dichiarazioni rese, risulta lecito. Occorre infatti sottolineare, sul piano generale, che l'identificazione certa e rigorosa dell'utenza, già richiesta alle banche in un'ottica di sana e prudente gestione del rischio, rappresenta, sovente, anche un obbligo posto in capo a tutti gli istituti di credito da specifiche normative di settore la cui violazione, peraltro, può costituire fonte di eventuale responsabilità civile".

⁸² Tribunale di Roma, sentenza n. 1127 del 23 gennaio 2017, in *Ilprocessotelematico.it* 2017. Il tribunale capitolino, nella specie, ha dichiarato la nullità di un contratto di compravendita di quote di società a responsabilità limitata sottoscritto con una firma digitale abusivamente utilizzata, cioè senza il consenso del titolare della smart card contenente il dispositivo che consente di apporre tale firma. Nella specie, il titolare della firma digitale ha dato prova che, nel giorno e nell'ora in cui l'atto di cessione risultava firmato digitalmente – e al quale era stata apposta la marca temporale – si trovava in luogo incompatibile con quello nel quale risultava sottoscritto il contratto.

⁸³ Con le cosiddette "firme" elettroniche o digitali si è passati da un modello basato sull'autorialità ad un modello basato sulla responsabilità e affidamento, in ordine all'utilizzo e alla diligente custodia. Si può, infatti, ritenere che colui che operi con strumenti informatici debba far fronte alle conseguenze che essi provocano e agli affidamenti che possano ingenerare (G. FINOCCHIARO, *Il contratto nell'era dell'intelligenza artificiale*, in *Riv. trim. dir. e proc. civ.*, 2018, 2, 441).

⁸⁴ Dalle tecniche di pseudonimizzazione vanno distinte quelle di anonimizzazione che si riferiscono a trasformazioni più radicali e definitive dei dati, tali per cui essi non si riferiscano ad una persona fisica identificata o identificabile o a dati resi sufficientemente anonimi da impedire o da non consentire più l'identificazione degli interessati. A tal riguardo il considerando n. 26 del GDPR dispone che "è auspicabile applicare i principi di protezione dei dati a tutte le informazioni relative a una persona fisica identificata o identificabile. I dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile. Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici. I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca".

⁸⁵ Regolamento CE, Parlamento Europeo n. 679 del 27 aprile 2016 (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE), in *G.U.U.E.* L 119/1 del 4 maggio 2016.



vate separatamente e sono assoggettate a misure tecniche e organizzative volte a garantire che tali dati non siano attribuiti a una persona fisica identificata o identificabile⁸⁶. Con la conseguenza che, ragionando *a contrario*, attraverso l'utilizzo delle suddette informazioni aggiuntive, le persone fisiche possono essere facilmente identificate.

Il GDPR all'art. 5, paragrafo 1, lettera c), stabilisce che i dati trattati devono essere “adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (c.d. minimizzazione dei dati)”. Essi, inoltre, devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (art. 5, paragrafo 1, lettera e)⁸⁷. Il GDPR, ai fini della disciplina in questione, individua, accanto al soggetto titolare del trattamento ossia “la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali” (art. 4, numero 7); anche il responsabile del trattamento individuabile “nella persona fisica o giuridica, nell'autorità pubblica, nel servizio o in altro organismo che tratta dati personali per conto del titolare del trattamento” (art. 4, numero 8). Avuto riguardo ai sistemi di blockchain, gestiti per definizione da più partecipanti, la individuazione di questi ruoli può presentare alcune difficoltà a seconda che si utilizzi il sistema *permissioned* o *permissionless*. Nei sistemi autorizzati *permissioned*, comprendenti un numero limitato di utenti, se questi non partecipano alla definizione delle regole assumono il ruolo di meri *data processor*; viceversa, ove gli utenti abbiano deciso le regole di convalida dei dati, si configura in capo a ciascuno di essi la figura di contitolari dei dati. I contitolari dei dati “determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14, a meno che, e nella misura in cui, le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti” (art. 26, paragrafo 1, del GDPR). I titolari del trattamento così individuati obbligati in base al principio di “responsabilizzazione” a garantire la tutela della persona e dei suoi dati secondo quanto predisposto dal paragrafo 1 dell'art. 5 del GDPR, devono essere anche in grado di provarlo (art. 5, paragrafo 2). Essi, perciò, devono mettere in atto tutte le misure tecniche e organizzative adeguate, eventualmente anche quelle ricomprese nell'art. 32 del GDPR⁸⁸ “per garantire che il tratta-

⁸⁶ Sul punto: N. BOLDRINI *Blockchain e GDPR: le sfide (e le opportunità) per la protezione dei dati*, in <https://www.blockchain4innovatio.it>; G. CORVI, *Smart contract, la sfida del GDPR*, in *Insurance review*, 2019, 24 ss.; A.M. GAMBINO, C. BONPREZZI, *Blockchain e protezione dei dati personali*, in *Dir. inf. e inform.*, 2019, 619, 619.

⁸⁷ L'art. 5 lettera e) statuisce, inoltre, che “i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato (limitazione della conservazione)”.

⁸⁸ L'art. 32 del GDPR prevede che “1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. 2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. 3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. 4. Il titolare del tratta-



mento è effettuato conformemente al regolamento” (art. 24 GDPR). Qualora i titolari del trattamento non operino in conformità a quanto previsto rispondono del danno cagionato ai sensi degli art. 82, paragrafo 2, GDPR. I responsabili del trattamento, invece, rispondono per il danno causato solo se non hanno adempiuto gli obblighi del regolamento specificatamente diretti ai responsabili del trattamento o hanno agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento (art. 82, paragrafo 2, GDPR).

Negli *smart contract* che utilizzano la tecnologia blockchain *permissionless* la individuazione dei titolari e, in subordine, dei responsabili del trattamento è decisamente più complessa poiché i soggetti non sono identificabili a priori e chi tratta i dati lo fa senza alcun permesso in quanto gli stessi sono irrimediabilmente pubblici. Una blockchain *permissionless* è accessibile a tutti, *open source* e trasparente; in essa manca qualsiasi meccanismo correttivo di discriminazione sui nodi della rete⁸⁹, “non vi è alcuna limitazione sui diritti di lettura e scrittura in mancanza di fiducia tra le parti, che permane solo nella piattaforma e nella crittografia, in modo che siano abilitate validazioni c.d. *trustless*” (senza fiducia)⁹⁰. Così mentre una prima più complessa soluzione individua tutti i nodi come contitolari (se determinano le finalità e i mezzi del trattamento) o responsabili (se agiscono per conto altrui) o, ancora, titolari per sé e responsabili per gli altri⁹¹; altra, invece, indica quale titolare del trattamento lo sviluppatore del *software*. Ma anche quest’ultima soluzione può apparire problematica perché in concreto lo sviluppatore del software può, in taluni casi, limitarsi a fornire soluzioni senza determinare finalità e mezzi del trattamento e quindi non diventare il titolare, mentre, in altri casi, può esserne semplicemente il responsabile⁹². Comunque, la individuazione del titolare del procedimento, può non giovare perché, in considerazione dell’immodificabilità, inalterabilità e persistenza dei dati che connotano la blockchain, alcuni diritti che l’interessato può far valere ai sensi del Regolamento 679/2016, sono inattuabili. Si pensi, in particolare, al diritto di rettifica e di integrazione dei dati (art. 16) ed al diritto alla cancellazione ed all’oblio (art. 17)⁹³. Inoltre, i caratteri di decentralizzazione, disintermediazione e distribuzione propri della blockchain mal si conciliano con il diritto alla limitazione di trattamento (art. 18) ed il diritto di opposizione al trattamento (art. 21) che erano stati formulati e concepiti dal legislatore per trattamenti centralizzati di dati⁹⁴. La blockchain, infatti, per il

mento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell’Unione o degli Stati membri”.

⁸⁹ In informatica e telecomunicazioni un nodo è un qualsiasi dispositivo hardware del sistema in grado di comunicare con gli altri dispositivi che fanno parte della rete; può quindi essere un computer, una stampante, un fax, un modem ecc. In ogni caso il nodo deve essere dotato di una scheda di rete. I nodi sono collegati tra loro da un pannello di connessione (in inglese *Hub*), chiamato anche *concentratore*, che ha la funzione di semplificare la connessione fisica tra i vari nodi e di instradare i segnali che vengono inviati da un nodo all’altro.

⁹⁰ M.T. GIORDANO, *La blockchain ed il trattamento dei dati personali*, in AA.VV., *Blockchain e smart contract*, cit., 107.

⁹¹ W. MAXWELL, J. SALMON, *A guide to blockchain and data protection*, Bruxelles, 2017, 11; M. FINK, *Blockchains and Data Protection in the European Union*, in *European data protection law review*, 2018, 4, 17. Criticamente F. FAINI, *Blockchain e diritto: la “catena del valore” tra documenti informatici, smart contracts e data protection*, in *Resp. civ. prev.*, 2020, 1, 297, secondo cui “tale interpretazione determina una conseguente difficoltosa individuazione pratica degli stessi e una correlata problematica distribuzione di responsabilità, che rischia di compromettere l’efficacia della tutela offerta dalla disciplina in materia di *data protection*; peraltro in tal caso risulta difficile individuare la determinazione “congiunta” delle finalità e dei mezzi del trattamento posta come condizione normativa necessaria a qualificare i soggetti come contitolari dall’art. 26 del Regolamento (UE) 2016/679. Anche nelle varianti interpretative che li indicano quali responsabili, questi lo sarebbero de facto, mancando il previsto atto di designazione da parte del titolare”.

⁹² M. GIULIANO, *La blockchain e gli smart contracts nell’innovazione del diritto nel terzo millennio*, in *Dir. inf. e inform.*, 2018, 989 ss.

⁹³ Sul punto A. DI LANDRO, *Big Data. Rischi e tutele nel trattamento dei dati personali*, Napoli, 2020.

⁹⁴ SARZANA S. DI F. IPPOLITO-M. NICOTRA, *Diritto della blockchain, intelligenza artificiale e Iot*, Torino, 2018, 68.



tramite di un qualsiasi *block explorer*, consente a chiunque l'accesso ai dati conservati nelle transazioni e nei blocchi senza alcun limite temporale.

Con l'intento di risolvere a monte il problema della individuazione dei soggetti titolari e/o responsabili del trattamento dei dati, la CNIL (*Commission nationale de l'informatique et des libertés*)⁹⁵ in un documento esplicativo emesso nel novembre del 2018 e intitolato "*Blockchain and the GDPR: solutions for a responsible use of the blockchain in the context of personal data*" ha ritenuto di potere applicare nella maggioranza dei casi l'esenzione di cui all'art. 2, comma 2, lettera c) del GDPR per i trattamenti c.d. personali o domestici. L'applicazione di questa esenzione consente di non far ricadere i trattamenti svolti dai privati sotto l'egida del GDPR e, pertanto, di non dovere considerare i nodi (non gestiti da utenti non professionali) quali responsabili del trattamento.

7. – Una volta che il testo del contratto sia stato tradotto in dati (anche da un redattore terzo estraneo al rapporto) e che sia stato firmato dalle parti secondo le modalità indicate, lo *smart contract* viene inserito in un blocco (identificato da un codice *hash*⁹⁶) contenente altre transazioni il quale, non appena viene *minato* (quando cioè viene risolto l'enigma matematico associato al codice del blocco, con conseguente controllo e validazione di ogni transazione) è aggiunto in maniera permanente e immutabile alla blockchain, accompagnato da una marca temporale che identifica in modo univoco la data e l'ora della transazione⁹⁷. Questa fase corrisponde a quella della esecuzione dello *smart contract*. Nel registro linguistico proprio dell'informatica il termine *execution* significa, infatti, "*performance of an instruction or program*" ossia avvio del programma che implica anche la lettura delle istruzioni caricate, l'accesso a particolari ambienti web con credenziali di autenticazione e la validazione del software sulla blockchain.

Dal momento della esecuzione (in senso informatico) del contratto, esso diventa vincolante per le parti (art. 8-ter del d.l. n. 135/2018)⁹⁸. Mentre nella ricostruzione tradizionale il contratto si conclude quando il proponente viene a conoscenza dell'accettazione di controparte (art. 1326 cod. civ.) e da questo momento diventa per esse vincolante (art. 1372 cod. civ.), lo *smart contract*, invece, vincola le parti solo all'atto della sua esecuzione. Le parti, consentendo in modo non equivoco alla esecuzione (in senso informatico) dello *smart contract*, lo rendono per esse vincolante⁹⁹. Da questo momento lo *smart contract*, dal punto di vista funzionale, è irretrattabile (in quanto una volta importato e validato sulla blockchain non può essere rimos-

⁹⁵ La CNIL è un'autorità amministrativa indipendente francese creata nel 1978 e incaricata di assicurare l'applicazione della legge sulla tutela dei dati personali nei casi in cui si effettuino raccolte, archiviazioni ed elaborazioni di dati personali.

⁹⁶ In informatica, l'*hash* è una funzione (o un algoritmo matematico) che svolge un compito ben preciso: in pratica, trasforma una qualsiasi stringa di lunghezza arbitraria in una stringa di lunghezza predefinita. Ad esempio, la locuzione "firma digitale", in Adler32 risulta così: 288e0573. L'*output* restituito da una funzione di *hash* si chiama *digest*. Al giorno d'oggi, esistono diverse funzioni crittografiche di *hash*. Si distinguono tra loro per il livello di sicurezza che garantiscono e per il tipo di *output* (o *digest*) che restituiscono. L'Adler32 è, appunto, una di esse. Tra le funzioni crittografiche di *hash* più diffuse e utilizzate, ci sono MD5 e SHA-1.

⁹⁷ La blockchain, oltre che immutabile, è altresì un registro trasparente. Ogni transazione è tracciata, sempre rintracciabile e liberamente consultabile da chiunque, anche se la mancanza di un obbligo per le parti di identificarsi mediante il proprio vero nome potrà garantire un anonimato di fatto o, come viene definito, uno pseudonimato, nel senso che è possibile individuare l'indirizzo informatico delle parti ma non la loro identità (G. CORVI, *Smart contract. La sfida del GDPR*, in *Insurance review*, 2019, 24 ss.).

⁹⁸ L'art. 8-ter del d.l. n. 135 del 14 dicembre 2018, cit., convertito in l. n. 12 dell'11 febbraio 2019, in *G.U.* n.36 del 12 febbraio 2019 (Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione).

⁹⁹ MANENTE, L. 12/2019 – *smart contract e tecnologie basate su registri distribuiti – prime note del Consiglio Nazionale del Notariato – Area informatica*, in *Studio I-2019 DI*, 2019, secondo cui "l'accordo sugli effetti è un momento antecedente da non confondere con l'esecuzione (in senso tecnico) dello *smart contract*".



so), immodificabile (poiché non vi è modo di intervenire per eliminare o modificare il contenuto di uno *smart contract*) e inarrestabile (poiché non può essere bloccata la sua esecuzione ed il conseguente adempimento delle operazioni economiche secondo le istruzioni fornite *ab initio*)¹⁰⁰. Il contratto che risulta esattamente eseguito (in senso informatico) produce effetti tra le parti (o se prestabilito a favore di terzi)¹⁰¹. In virtù del meccanismo “... *if ... then ...*”, così come già rilevato nel caso dello *smart contract* esecutivo, le parti possono subordinare l’efficacia del negozio ad una condizione o ad un termine, ovvero possono utilizzare l’algoritmo per cautelarsi anticipatamente dal rischio di inadempimento contrattualizzando l’*exceptio inadimpleti contractus*.

Solo dopo avere prodotto i suoi effetti lo *smart contract* si disattiva, ma non sparisce del tutto restando nel blocco in cui era stato originariamente inserito. Per ovviare a ciò, l’unica possibilità che i sistemi più avanzati (ad esempio Ethereum) forniscono è la introduzione nella blockchain della c.d. funzione *kill* o di autodistruzione che punta a rimuovere i programmi non più impiegati, con la finalità di efficientare le *performance* della *blockchain*. Tale funzione è attivabile solo dal nodo che ha creato lo *smart contract* o attraverso l’inoltro di una transazione e immettendo nella *blockchain* il corrispondente codice elettronicamente firmato dalle parti, ovvero attraverso la predisposizione di un accordo *a latere* in cui i contraenti abbiano previsto i casi di attivazione della medesima¹⁰².

8. – Dall’analisi empirica condotta sembra possa trarsi una prima conclusione. Lo *smart contract* può essere sia lo strumento attraverso il quale le parti veicolano una volontà già formatasi (*smart contract* con funzione strumentale o con funzione esecutiva), sia l’unico mezzo tramite il quale i contraenti oggettivizzano la sequela di effetti e prestazioni che si siano vicendevolmente promessi (*smart contract* con funzione costitutiva). Nell’ambito del procedimento di stipulazione del contratto tramite *smart contract*, indipendentemente dalla funzione che esso riveste, ci troviamo di fronte ad un fenomeno che prevede due o più parti che agiscano secondo comuni intenzioni; tali intenzioni (volontà) si incontrano dando luogo ad un assetto di interessi e di prestazioni; tale assetto, mediante l’adempimento dei rispettivi obblighi, genera degli effetti che ineriscono (costituendolo, modificandolo o estinguendolo) un rapporto giuridico patrimoniale (art. 1321 cod. civ.). Lo svolgimento fisiologico del rapporto contrattuale che si sviluppi tramite *smart contract*, a differenza di quanto accade per i contratti tradizionali, difficilmente può essere ostacolato da problematiche intrinseche allo stesso (vizi e/o altre cause di invalidità) o da fattori esterni che influiscano negativamente sull’andamento di quanto le parti avevano previsto. A differenza dei contratti tradizionali che possono essere colpiti da nullità qualora manchi uno degli elementi essenziali, o ricorra l’illiceità della causa, la illiceità dei motivi o manchi-

¹⁰⁰ S. CERRATO, *Contratti tradizionali, diritto dei contratti e smart contract*, in AA.VV., *Blockchain e smart contract*, Milano, 2019, 301, secondo cui ci “troviamo al cospetto di un *tertium genus* di formazione del contratto che si aggiungerebbe al meccanismo della consensualità (contratto che si conclude con l’incontro dei consensi) e della realtà (contratto che si conclude con la traditio della cosa); il contratto che si conclude per effetto della validazione diffusa da parte dei nodi della blockchain”.

¹⁰¹ Lo *smart contract* può veicolare un contratto a favore di terzo (art. 1411 ss. cod. civ.). In tal caso stipulante e promittente possono inserire opportune linee di codice che indirizzino le prestazioni da attuare verso l’ulteriore destinatario, il quale può aderire alla stipulazione sottoscrivendo a sua volta il contratto in formato smart. Non è compatibile con il protocollo dello *smart contract* la designazione successiva del contraente (artt. 1401 ss. cod. civ.), a meno di non congegnare il meccanismo di elezione del terzo come input proveniente da un oracolo agente sotto il controllo dello stipulante. Il nominato deve, per poter validamente subentrare nel rapporto contrattuale, accettare contestualmente la nomina apponendo la propria sottoscrizione in via informatica.

¹⁰² A. CONTALDO, F. CAMPARA, *Blokchain criptovalute, smart contract, industria 4.0. Registri digitali, accordi giuridici e nuove tecnologie*, Pisa, 2019, 9.



no, con riferimento all'oggetto, i requisiti di possibilità, liceità, determinatezza o determinabilità (art. 1418 cod. civ.), lo *smart contract* non può essere affetto da tali cause di invalidità.

In un contratto redatto tramite *smart contract* è, infatti, inimmaginabile che possa mancare l'accordo. La volontà delle parti opera in un momento iniziale in cui i contraenti decidono di ricorrere allo strumento tecnologico per lo svolgimento dell'attività contrattuale; nel momento in cui i soggetti si avvalgono dello strumento tecnologico per integrare la propria volontà nella formazione del regolamento di interessi definitivo; ed, infine, la volontà emerge con riguardo agli effetti, giacché il contraente intende utilizzare le tecnologie non solo per giungere al perfezionamento di un contratto senza il suo diretto controllo, ma anche per goderne degli effetti giuridici¹⁰³. Una volta che lo *smart contract* venga attivato, esso esce dalla sfera di controllo delle parti e la gestione del rapporto contrattuale avviene in maniera automatica¹⁰⁴.

Parimenti è impensabile che in uno *smart contract* possano mancare la causa e l'oggetto¹⁰⁵, necessariamente enunciati dalle parti: se dovessero mancare lo *smart contract* non si "autoeseguirebbe". L'eventuale illiceità della causa o dei motivi e l'illiceità dell'oggetto possono essere, invece, rilevate mediante l'azione di un oracolo che permetta allo *smart contract* di ottenere informazioni dal mondo esterno e che garantisca che le informazioni siano giuste e veritiere. Un caso limite è rappresentato dallo *smart contract* contrario a norme imperative. Si presume, infatti, che in tale circostanza l'autore si guarderà bene dal programmare il suo *smart contract* in modo tale che esso cessi di avere efficacia, se non altro perché la sua intenzione, con molta probabilità, era quella di conseguire, a mezzo del contratto, un risultato contrario a norme di legge.

Anche la forma è elemento essenziale dello *smart contract*. Nella specie, quella dello *smart contract* è da considerarsi forma scritta rappresentativa della volontà delle parti, conservabile su un supporto durevole ed intellegibile dalla comunità virtuale che lo utilizza. Il linguaggio informatico è costituito da lemmi informatici codificati: ad un comando o elemento corrisponde un significato ed un effetto¹⁰⁶.

9. – Anche con riguardo alle cause di annullabilità occorre precisare che, su un contratto *self-executing* qual è lo *smart contract*, esse non sembrano in buona parte ipotizzabili¹⁰⁷. Certamente non lo sono né l'occultamento della minore età, difficile da ipotizzare quando dialogano tra loro due *smart contract*¹⁰⁸, né

¹⁰³ F. BRAVO, *Contratto cibernetico*, in *Dir. informatica*, 2, 2011, 169 ss.

¹⁰⁴ N. GENTILE, *Vicende patologiche del contratto in forma di smart contract*, in AA.VV., *Blockchain e smart contract*, cit., 321, secondo il quale ci si trova in un contesto in cui vi è la massima predeterminazione possibile del dettato contrattuale e di detto dettato è fatta esecuzione in maniera automatica e irrettabile ... è essenziale che il meccanismo dello *smart contract* non preveda altro se non un perfetto combaciare di proposta e di accettazione, tradotto in linguaggio di codice informatico".

¹⁰⁵ Né può prospettarsi l'ipotesi di uno *smart contract* con oggetto impossibile o indeterminato. L'oggetto deve essere possibile se non altro perché, in caso contrario, il contratto non avrebbe risultati nel mondo reale al quale fosse collegato. La sopravvenuta possibilità dell'oggetto, essendo una vicenda esterna allo *smart contract*, dovrà essere portata a conoscenza del sistema operativo. "Lo *smart contract* che voglia godere di tale comunicazione e, a seguito ed in forza di essa, divenire operativo e superare il blocco, dovrà essere aperto a tale comunicazione ed essere in grado di comprenderla e recepirla". L'oggetto deve essere, altresì, determinato e devono esserlo le prestazioni necessarie a conseguirlo o ad esso correlate. Il fatto che lo *smart contract* sia un contratto deterministico implica, infatti, la circostanza che "la fase del conseguimento delle azioni attese (e dei loro risultati) venga spostata nell'ambito della eventualità e della interpretazione suppletiva a cui solo successivamente segua l'azione vera e propria" (N. GENTILE, *Vicende patologiche del contratto in forma di smart contract*, in AA.VV., *Blockchain e smart contract*, cit., 322 e 323).

¹⁰⁶ Con riferimento al problema della forma del contratto informatico si veda *supra* "Smart contract con funzione costitutiva del contratto. Formazione ed intellegibilità del vincolo".

¹⁰⁷ S. CRISCI, *Intelligenza artificiale ed etica dell'algoritmo*, in *Foro amm.*, 2018, 1787.

¹⁰⁸ Non esiste ad esempio un'età legale per acquistare criptovaluta Bitcoin. (addirittura molti siti insegnano ai minorenni come



la violenza ed il dolo, inconciliabili con l'automatismo proprio di questa tipologia contrattuale e semmai riferibili al contratto preliminare con il quale le parti hanno scelto di adottare la forma cibernetica per le loro transazioni¹⁰⁹. Violenza e dolo potrebbero, se del caso, essere esercitati sul programmatore che si occupa della installazione del *software*. Se sul programmatore è usata violenza, non essendovi da parte del contraente la possibilità di operare una consapevole scelta sull'opportunità di evitare il male minacciato poiché la minaccia non è rivolta alla sua persona (art. 1435 cod. civ.), non appare applicabile alla suddetta ipotesi la normativa sull'annullabilità del contratto. Se, invece, sul programmatore vengono esercitati raggiri, bisogna distinguere a seconda dell'identità del soggetto che li ha posti in essere. Se si tratta della controparte che ha raggirato il programmatore al servizio dell'altro contraente, questi, ove i raggiri fossero stati decisivi per la conclusione del contratto, potrebbe chiederne l'annullamento ai sensi dell'art. 1439, comma 1, cod. civ. Se, invece, l'autore del dolo è un terzo potrà applicarsi il secondo comma dell'art. 1439 cod. civ., in cui è sancita l'annullabilità del contratto, solo se i raggiri posti in essere dal terzo siano conosciuti dal contraente che ne ha tratto vantaggio¹¹⁰.

A differenza della violenza e del dolo, l'errore può inficiare la validità dello *smart contract* ma, ai sensi dell'art. 1428 cod. civ., devono ricorrere i requisiti della essenzialità e della riconoscibilità. È essenziale l'errore determinante del volere, ossia in assenza del quale il contraente non avrebbe concluso il negozio; è riconoscibile, invece, quando una persona di normale diligenza, tenendo conto delle circostanze, riuscirebbe a rilevarlo. Tralasciando l'essenzialità, la cui verifica non crea particolari problemi in relazione a questo tipo di contratti, l'aspetto della riconoscibilità induce ad alcune riflessioni. In considerazione, infatti, del disposto di cui all'art. 1431 cod. civ. secondo cui l'errore si considera riconoscibile quando, "in relazione al contenuto, alle circostanze del contratto, ovvero alla qualità dei contraenti, una persona di normale diligenza avrebbe potuto rilevarlo", è necessario operare un netto distinguo a seconda che il contraente destinatario del messaggio veicolato attraverso uno *smart contract* operi o meno nell'esercizio di un'attività professionale. Se il contraente che riceve il messaggio sia un professionista, al fine di analizzare il requisito della riconoscibilità, è a lui richiesto uno sforzo maggiore di quello preteso da una persona "comune". E ciò in considerazione del fatto che il contraente professionale può comprendere con più facilità i procedimenti logici che il programma svolge e studiarne gli algoritmi. Secondo quanto previsto dall'art. 64-bis della l. 22 aprile 1941 n. 633 sul diritto d'autore, l'utente, infatti, può "osservare, studiare o sottoporre a prova il funzionamento del programma, allo scopo di determinare le idee ed i principi su cui è basato ogni elemento del programma stesso, qualora egli compia tali atti durante operazioni di caricamento, visualizzazione, esecuzione, trasmissione o memorizzazione del programma che egli ha il diritto di eseguire", senza violare alcun diritto di proprietà intellettuale. L'utente professionale, dunque, che pone in essere tali operazioni può agevolmente rilevare gli eventuali vizi presenti nello *smart contract* e richiederne l'annullamento. La legge prescrive che, però, la parte caduta in errore non può chiedere l'annullamento del contratto se, prima che ad essa possa derivarne pregiudizio, l'altra offra "di eseguirlo in modo conforme al contenuto e alle modalità del contratto che quella intendeva concludere" (art. 1432 cod. civ.). Uno *smart contract* aperto ad una proposta di modifica unilaterale consentirà di salvaguardare l'attività contrattuale svolta e le intenzioni delle parti.

Se l'utente è, invece, soggetto che non conosce il linguaggio informatico o i procedimenti logici che in-

acquistare bitcoin si veda per esempio <https://www.investmentimagazine.it/>). Solo alcuni scambi di criptovaluta impongono un'età minima di diciotto anni.

¹⁰⁹ M. IECHER, *I vizi del consenso nel contratto cibernetico*, in <https://www.jei.it/approfondimenti-giuridici>.

¹¹⁰ R. CLARIZIA, *Informatica e conclusione del contratto*, Milano, 1985, 132.



ducono il computer a generare la dichiarazione e non è capace di compiere le eventuali operazioni di *reverse engineering*¹¹¹, sarà pressoché impossibile per lui accorgersi di eventuali errori nell'elaborazione o nella trasmissione dello *smart contract*. L'utente non professionale, perciò, non potrà far nulla se l'errore non risulta riconoscibile dal testo trasmesso o da altre forme di *output*¹¹². Se l'errore non è riconoscibile, il rischio di eventuali divergenze tra la volontà originaria e quanto espresso dall'elaboratore potrebbe attribuirsi al *dominus* del computer, in ossequio al principio dell'affidamento in buona fede per salvaguardare gli scambi e secondo il brocardo "*cuius comoda, cuius incomoda*"¹¹³, quale prezzo da dover pagare per i benefici che derivano dall'utilizzo del computer, sia in termini di risparmio di tempo che di incremento del volume di affari. Anche in questa materia, dunque, riveste un ruolo importante la teoria dell'affidamento per salvaguardare la circolazione dei beni, e va sottolineato come esista negli *smart contract* un rischio più elevato per i contraenti non professionisti che, comunque, è consapevolmente accettato nel momento della scelta di affidare la conclusione di una transazione ad un elaboratore.

Discorso a parte va fatto, infine, per l'errore di calcolo (art. 1430 cod. civ.). Con riguardo agli *smart contract*, quando si parla di "errori di calcolo" può farsi riferimento oltre che agli errori aritmetici che vengono facilmente rilevati dal sistema e rettificati automaticamente, anche alle operazioni effettuate dall'elaboratore sulla base delle istruzioni impartite al programma¹¹⁴. Anche in questo caso, ove le suddette sviste nel codice non siano alla base di algoritmi fondamentali, può procedersi a semplice rettifica del contratto. Naturalmente più semplice è il contratto cui la macchina deve attendere, minori sono le combinazioni di istruzioni che devono essere fornite e, conseguentemente, minori sono le possibilità di errori.

10. – In presenza di gravi errori di progettazione (*bugs*)¹¹⁵ del programma o se la blockchain non sia perfettamente funzionante tanto da generare errori di programmazione, lo *smart contract* potrebbe portare i con-

¹¹¹ Il reverse engineering viene anche denominato "back engineering", ovvero "progettazione all'incontrario". Effettuato generalmente in due fasi, il reverse engineering consiste nell'identificazione dei componenti del sistema e delle loro relazioni, quindi delle loro rappresentazioni a un livello di astrazione più elevato e più comprensibile dall'uomo (specifiche, documentazione, piani, diagrammi). Ciò non comporta la modifica o la creazione di un nuovo sistema basato su questo reverse engineering. È un processo di analisi, non di alterazione o replica. Il risultato di questa analisi può essere particolarmente vantaggioso o completamente inutilizzabile, a seconda della persona che esegue il reverse engineering e della sua conoscenza dell'oggetto in studio. Questi risultati saranno tanto più vantaggiosi grazie all'utilizzo di strumenti dedicati e il futuro del reverse engineering si baserà sull'evidenza dell'efficacia di questi metodi e strumenti in un dato contesto.

¹¹² Mentre gli input sono i dati che il programma riceve in ingresso, gli output, invece, sono i dati che il programma trasmette verso un soggetto terzo. Anche i dati salvati su disco rigido sono output dato che vengono inviati al gestore delle periferiche che provvede a memorizzarli nella memoria magnetica.

¹¹³ R. BORRUSO, G. CIACCI, *Diritto civile e informatica*, Napoli, 2004, 226.

¹¹⁴ M. PENNASILICO, *La conclusione dei contratti on line tra continuità e innovazione*, in *Diritto dell'informatica*, 2005, 6, 805 ss.

¹¹⁵ Nel gergo informatico la parola *bug* (letteralmente "insetto") identifica un errore in un programma software; meno comunemente, il termine *bug* può indicare un difetto di progettazione in un componente hardware che ne causa un comportamento imprevisto o comunque diverso da quello specificato dal produttore. L'uso del termine *bug* secondo alcuni risale ad un curioso aneddoto risalente al 1945 quando il tenente Hopper ed il suo gruppo, cercando la causa del malfunzionamento di un computer "*Mark II*", si accorsero che una falena si era incastrata tra i circuiti. Dopo aver rimosso l'insetto, il tenente incollò la falena rimossa sul registro del computer e annotò: "*1545. Relay #70 Panel F (moth) in relay. First actual case of bug being found*". Questo registro è conservato presso lo Smithsonian National Museum of American History. In realtà, si ritiene che già Thomas Edison utilizzò il termine. Ne è prova una lettera scritta il 13 novembre 1878 ad un suo amico in cui egli si riferisce a piccoli errori e difficoltà chiamandoli *bugs* ("*It has been just so in all of my inventions. The first step is an intuition, and comes with a burst, then difficulties arise—this thing gives out and [it is] then that Bugs—as such little faults and difficulties are called—show themselves and months of intense watching, study and labor are requisite before commercial success or failure is certainly reached*").



traenti (o anche uno di essi) a confrontarsi con risultati molto dissimili da quelle che erano le loro (sue) iniziali previsioni. Che la blockchain, pur sottoposta a pesanti sessioni di *testing*, possa essere malfunzionante nonostante ne siano sottolineati i caratteri di sicurezza ed inalterabilità dei dati¹¹⁶, è un fatto pressoché condiviso. Lo dimostra la circostanza che, ove l'utente decida di effettuare il *download* del programma che consente di utilizzare la piattaforma, egli debba preliminarmente accettare alcune clausole di integrale esonero da responsabilità del gestore. Spesso, poi, la sottoscrizione di tali clausole è accompagnata dalla scelta compiuta dall'utente del *rimedio*¹¹⁷ da adottare in caso di malfunzionamento del sistema (*hard e soft fork*)¹¹⁸. Sottoscrizione delle clausole e scelta dei rimedi da parte degli utenti dimostrano, evidentemente, che l'utilizzo della piattaforma può implicare potenziali rischi informatici a carico dell'utente.

Il creatore-gestore della blockchain, pur non essendo obbligato a controllare le operazioni compiute sulla piattaforma¹¹⁹, deve, garantire la massima sicurezza del servizio tecnologico messo a disposizione degli utenti sì da impedire che esso produca effetti pregiudizievoli¹²⁰. In mancanza di una apposita disciplina¹²¹, è ragionevole ritenere che qualora l'utente subisca un danno (ad esempio furto di criptomoneta¹²² o di altri beni), i gestori di blockchain ne siano responsabili¹²³. Poiché il funzionamento decentralizzato della blockchain implica che il gestore non abbia il controllo delle operazioni compiute (il che già esclude una responsabilità fondata sulla colpa), è ragionevole ritenere che un eventuale danno subito dagli utenti per il malfunzionamento della piatta-

¹¹⁶ F. PILKINGTON, *Blockchain Technology: Principles & Applications*, in AA.VV., *Research Handbook on Digital Transformations*, Cheltenham, 2016, 15.

¹¹⁷ Sul concetto di rimedio si veda Y. ADAR, P. SIRENA, *La prospettiva dei rimedi nel diritto privato europeo*, in *Riv. dir. civ.*, 2012, I, 359 ss.

¹¹⁸ La scelta compiuta dagli utenti si risolve nell'alternativa tra *hard e soft fork* della piattaforma blockchain. Gli *hard fork* sono aggiornamenti software non retrocompatibili. Tipicamente, si verificano quando i nodi aggiungono nuove regole in conflitto con le regole dei vecchi nodi. I nuovi nodi possono comunicare solo con altri che usano la nuova versione. Di conseguenza, la blockchain si divide, creando due network separati: uno con le vecchie regole e uno con le nuove regole. Un *soft fork* è, invece, un aggiornamento *retrocompatibile*, ovvero i nodi aggiornati possono comunque comunicare con quelli non aggiornati. Ciò che vediamo tipicamente in un *soft fork* è l'aggiunta di una nuova regola che non si scontra con le regole più vecchie.

¹¹⁹ In ciò il gestore di blockchain si distingue dal *internet provider* che, ai sensi degli articoli 16 e 17 del Decreto legislativo n. 70 del 9 aprile 2003 (Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico, in *G.U.* n. 87 del 14 aprile 2003), se a conoscenza di elementi illeciti presenti sulla piattaforma, deve rimuoverli.

¹²⁰ V. WALCH, *The bitcoin blockchain as financial market infrastructure: a consideration of operational risk*, in *Journal of legislation and public policy*, 2015, 837.

¹²¹ Non vi è al momento una disciplina specifica che individui i profili di responsabilità dei gestori di piattaforme di blockchain. Sebbene la Commissione Europea abbia presentato la Proposta di direttiva sulla responsabilità dei fornitori di servizi del 20 dicembre 1990, essa, però, non ha avuto seguito nella legislazione successiva. In merito a tale proposta, si vedano: C. CASTRONOVO, *La responsabilità del prestatore di servizi nella proposta di direttiva comunitaria*, in *Foro it.*, 1994, V, 273; G. WAGNER, *Robot liability*, in <https://www.rewi.hu-berlin.de>, 2019, 36.

¹²² La criptomoneta è una rappresentazione digitale di valore, decentralizzata, basata sul peer-to-peer, su una Blockchain condivisa il cui trasferimento si fonda sulla crittografia e le cui regole di emissione sono basate su un algoritmo open source. La criptomoneta è, pertanto, un protocollo di comunicazione contenente in sé molto più che una moneta così come noi la intendiamo normalmente avendo insita al suo interno informazioni specificatamente programmate per un determinato uso: ad esempio la criptomoneta Ethereum è stata programmata per essere utilizzata nei c.d. *smart contract* mentre la cripto Monero, invece, per eseguire transazioni non tracciabili (F. BARTOLINI, *Requisiti della criptovaluta, ex art. 2464, comma 2, cod. civ., ai fini del conferimento nel capitale sociale di una s.r.l.*, in *IlSocietario.it*, 2018).

¹²³ Se si enfatizza l'idea che "the rules on tort are mainly based on the rationale that the liable person is the one who has created a risk which materialises in some manner of damage", può di conseguenza inferirsi il riconoscimento della responsabilità dei gestori creatori di una piattaforma blockchain, i quali sovente rivendicano la sicurezza da essa offerta, quantunque poi il relativo malfunzionamento non di rado si concretizzi in un danno economico per gli utenti (F. PATTI, *The European Road to Autonomous Vehicles*, in *Fordham International Law Journal*, 43, 2019, 150).



forma gravi su chi poteva evitarlo¹²⁴. In capo al gestore-creatore della piattaforma può, dunque, ipotizzarsi “una responsabilità di natura oggettiva”¹²⁵ che lo obbliga a risarcire i danni patiti dagli utenti. Il relativo peso economico del risarcimento è trasferito da chi lo ha subito al gestore che lo deve risarcire¹²⁶. Anche i dati provenienti dall’analisi economica avvalorano la conclusione secondo cui solo il creatore-gestore della piattaforma blockchain può sostenere il danno patito dagli utenti ed i costi derivanti¹²⁷. In ragione del fatto che gli *smart contract* conclusi con la blockchain sono destinati a diventare in futuro sempre più numerosi con un determinante incremento del rischio in capo al gestore della piattaforma, il Parlamento europeo nella Risoluzione del 16 febbraio 2017¹²⁸ ha invitato la Commissione a riflettere sull’opportunità di introdurre un meccanismo assicurativo obbligatorio per i sistemi autonomi e, dunque, anche per le tecnologie fondate sui registri distribuiti¹²⁹. La Commissione ha iniziato a lavorare su taluni profili evidenziati esitando il 25 aprile 2018 un primo documento di lavoro che mette in relazione le esistenti regole di responsabilità da prodotto difettoso con le tecnologie digitali esistenti. A questo primo atto è seguita il 7 maggio 2018 la Relazione della Commissione al Parlamento europeo, al Consiglio ed al Comitato economico e sociale europeo sull’applicazione della Direttiva del Consiglio relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri in materia di responsabilità per danni da prodotti difettosi (Direttiva 85/374/CEE), quale strumento di valutazione diretto a verificare l’efficacia della Direttiva stessa¹³⁰. In realtà è la già sussistente via della responsabilità oggettiva del produttore-gestore a essere ritenuta preferibile, in considerazione della agevolata posizione del soggetto danneggiato che deve dimostrare l’esistenza del danno e del difetto, unitamente al nesso causale tra difetto e danno¹³¹. Da questo punto di vista il richiamo all’assicurazione obbligatoria viene ritenuto “utile per consentire di affrontare, almeno temporaneamente, gli aspetti connessi alla responsabilità dal punto di vista economico”¹³². Con riferimento ai danni prodotti da un malfunzionamento della blockchain, in particolare, l’assicurazione obbligatoria avrebbe risvolti positivi sia per il gestore che può trasformare il rischio del servizio offerto in un costo prevedibile della sua attività¹³³, sia per gli utenti, i quali non incorrerebbero nella possibile mancata realizzazione dei propri interessi sottesi al credito risarcitorio. Ciò determinerebbe, quale ulteriore ef-

¹²⁴ C. CASTRONOVO, *Responsabilità civile*, Milano, 2018, IV, 439.

¹²⁵ C. LEANZA, *Intelligenza artificiale e diritto: ipotesi di responsabilità civile nel terzo millennio*, in *Resp. civ. prev.*, 2021, 3, 1011; N. BUONANNO, *La responsabilità civile nell’era delle nuove tecnologie: l’influenza della blockchain*, in *Resp. civ. prev.*, 2020, 1618.

¹²⁶ Il problema, in tale ambito, non deve essere tanto quello della individuazione del responsabile materiale del danno, bensì quello della identificazione delle condizioni di rilevanza del danno e dei criteri per l’addebito dei conseguenti obblighi (S. RODOTÀ, *Il problema della responsabilità oggettiva*, Milano, 1967, 73; P. TRIMARCHI, *Rischio e responsabilità oggettiva*, Milano, 1961, 16).

¹²⁷ R. DEMOGUE, *Fault, risk, and apportionment of loss in responsibility*, in *Illinois Law Review*, 1918, 308.

¹²⁸ Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, in *G.U. – C 252/239* del 18 luglio 2018.

¹²⁹ DE P. FILIPPI-A. WRIGHT, *Blockchain and the Law*, Harvard, 2019, 174.

¹³⁰ Nella Relazione, la Commissione ritiene la Direttiva “idonea a contribuire ad un ragionevole equilibrio tra la tutela dei danneggiati e la garanzia di una concorrenza leale sul mercato unico” (paragrafo 5.1), fondata sul concetto di responsabilità oggettiva “in virtù del quale i produttori sono responsabili dei prodotti difettosi indipendentemente dal fatto che il difetto sia o meno dovuto a colpa del produttore” (paragrafo 1). La Commissione, peraltro, si era impegnata a pubblicare a breve scadenza “orientamenti sulla Direttiva e una relazione sui quadri normativi in materia di responsabilità e sicurezza in relazione ALL’IA, all’internet delle cose e alla robotica, che ne indichi le implicazioni più ampie e le potenziali lacune e fornisca i relativi orientamenti. Se del caso la Commissione aggiornerà determinati aspetti della Direttiva, come i concetti di difetto, danno, prodotto e produttore. In principio generale di responsabilità oggettiva rimarrà tuttavia inalterato” (paragrafo 6).

¹³¹ Così E. PALMERINI, *Robotica e diritto, suggestioni, intersezioni, sviluppi a margine di una ricerca europea*, in *Resp. civ. prev.*, 2016, 1839.

¹³² E. PALMERINI, *Robotica e diritto, suggestioni, intersezioni, sviluppi a margine di una ricerca europea*, cit., 1842.

¹³³ DI D. SABATO, *Gli smart contract: robot che gestiscono il rischio contrattuale*, in *Contratto e impresa*, 2017, 399.



fetto riflesso, un beneficio collettivo in termini di fiducia degli utenti nei confronti di questa tipologia di mercato e del suo corretto funzionamento.

11. – L’irreversibilità delle transazioni effettuate mediante *smart contract* e l’automaticità dell’adempimento che si realizza a prescindere da un comportamento delle parti, non osta alla possibilità di prevedere, nei contratti a prestazioni corrispettive, la risoluzione per inadempimento¹³⁴. La fattispecie si presta alla collaborazione di una *library* (contenitore) di “variabili” che corrispondono a particolari “clausole contrattuali”. In questo caso la *library* può individuare i casi di inadempimento scritti su misura dello *smart contract*. Se la fattispecie di inadempimento risulta tra quelle comprese nella *library* e non ricade tra quelle pre-considerate di scarsa importanza (art. 1455 cod. civ.), essa è utilizzabile per attivare le conseguenze derivanti dall’inadempimento. Infatti, con l’algoritmo ... *if ... then ...* (se le variabili sono contenute nella *library* ... *allora* ...) è possibile prevedere, così come disposto dall’art. 1453 cod. civ., l’alternativa tra la scelta dell’adempimento e della risoluzione, o il blocco della possibilità di chiedere l’adempimento una volta che sia stata chiesta la risoluzione del contratto, o l’impossibilità di adempiere dopo la domanda di risoluzione. Anche il risarcimento del danno potrà essere integrato con tali mezzi: si pensi alla stipulazione di una clausola penale (art. 1382 cod. civ.) ed alla possibilità di ridurla se l’obbligazione principale sia stata in parte eseguita (art. 1384 cod. civ.), o alla individuazione di somme messe a disposizione (in riserva di eventuali danni) che possano essere liberate una volta che il sistema abbia accertato il diritto della parte ad ottenerle¹³⁵.

Come nei contratti basati sullo scambio istantaneo, l’utilizzo dello *smart contract* presenta numerosi vantaggi in termini di calcolabilità degli esiti della relazione negoziale, innanzitutto con riguardo alla riduzione, o comunque alla gestione, dell’inadempimento della controparte, altrettanto può dirsi nei contratti di durata¹³⁶ in cui assumono frequentemente rilevanza le c.d. sopravvenienze, cioè eventi imprevisi ed imprevedibili dalle parti al momento della stipulazione del contratto che incidono sull’equilibrio del sinallagma delle prestazioni. Occorre allora chiedersi se ed in che modo, attraverso gli *smart contract*, sia possibile garantire l’esecuzione della prestazione anche in presenza di accadimenti in origine non considerati dalle parti (quali ad esempio l’impossibilità sopravvenuta della prestazione e l’eccessiva onerosità della stessa)¹³⁷. Se il contratto è stato concluso mediante *smart contract* è prefigurabile la risoluzione del vincolo negoziale per impossibilità sopravvenuta della prestazione (art. 1463 ss. cod. civ.). Ciò può avvenire, ad esempio, se il bene cui la prestazione si riferisce sia stato tradotto nello *smart contract* in un *token*. Se il bene perisce nella sua

¹³⁴ L. PAROLA-P. MERATI-G. GAVOTTI, *Blockchain e smart contract: questioni giuridiche aperte*, in *Contratti*, 2018, 6, 687.

¹³⁵ Ciò permetterebbe alle parti di esperire rimedi di carattere restitutorio, adempiendo cioè ad una prestazione da eseguire in forma specifica o per equivalente, ove ciò sia possibile. Nel caso di prestazioni infungibili, la parte adempiente dovrebbe poter accedere alla chiave privata della controparte oppure alla password del computer in cui è conservata.

¹³⁶ Sul tema, a solo titolo esemplificativo, si vedano: E. GABRIELLI, *I contratti di durata, il diritto italiano e il nuovo codice civile argentino*, in *Giust. civ.*, 2018, 2, 267; G. OPPO, *Scritti giuridici. Obbligazioni e contratti*, Padova, 1992, 203; ID., *I contratti di durata*, in *Riv. dir. comm.*, 1943, I, 144; G. OSTI, *Contratto*, in *Nss. D.I.*, Torino, 1959, IV, 496 ss.; ID., *Clausola rebus sic stantibus*, in *Nss. D.I.*, Torino, 1959, III; ID., *Appunti per una teoria della “soprapvenienza” (La così detta clausola “rebus sic stantibus” nel diritto contrattuale odierno)*, in *Riv. dir. civ.* 1913, 471 ss.; ID., *La così detta clausola “rebus sic stantibus” nel suo sviluppo storico*, in *Giust. civ.*, 1912, 1; L. DEVOTO, *L’obbligazione ad esecuzione continuata*, Padova, 1943; G. STOLFI, *Appunti sui contratti di durata*, in *Studi in onore di B. Scorza*, Roma, 1940.

¹³⁷ G. NUZZO, *Gli smart contract tra esigenze di calcolabilità e gestione delle sopravvenienze*, in <https://www.economia.unimore.it>.



totalità, ne dà notizia al *token* che, a sua volta, trasmette questa informazione allo *smart contract*. Tale circostanza che, *ex lege*, libera la parte dall'obbligo di eseguire la prestazione, può dar luogo in uno *smart contract* ad un meccanismo di restituzione della eventuale controprestazione che sia stata (in tutto o in parte) ricevuta (art. 1463 cod. civ.). Se, invece, la prestazione è solo parzialmente impossibile, le informazioni trasmesse dal *token* allo *smart contract* abilitano il sistema ad una corrispondente riduzione (in numeri o proporzione) della controprestazione (art. 1464 cod. civ.)¹³⁸.

È, altresì, immaginabile che la risoluzione del contratto a prestazioni corrispettive veicolato dallo *smart contract* possa operare anche nel caso in cui la prestazione sia diventata eccessivamente onerosa per il verificarsi di avvenimenti straordinari ed imprevedibili (art. 1467 cod. civ.). Peraltro, pare innegabile che, a fronte di una domanda automatica di risoluzione del contratto, possa offrirsi, intra *smart contract*, la modifica delle condizioni di contratto in forza di una eccessiva onerosità conseguente ad un evento imprevedibile. Lo *smart contract*, infatti, può desumere questa informazione da un oracolo che, a sua volta, abbia assunto la notizia del verificarsi di detto evento ed abbia ricalcolato, in base a indici preinseriti, il valore della prestazione. La riduzione della prestazione o la modifica “nelle modalità di esecuzione, sufficienti per ricondurla ad equità” può essere richiesta anche se si tratta di un contratto nel quale una sola delle parti abbia assunto obbligazioni (art. 1468 cod. civ.).

12. – Azionabili con le stesse modalità sono le ipotesi di risoluzione di diritto. L'intimazione scritta che preveda un termine per l'adempimento (art. 1454 cod. civ.) può essere fatta partire dallo *smart contract* al verificarsi di un inadempimento “tracciato” di controparte. La decorrenza del termine rende automatica la risoluzione di diritto del contratto con la conseguenza che nessuna prestazione contrattuale è più effettuabile e, nei limiti di quanto prestabilito, lo *smart contract* può procedere alla riduzione in pristino ed al risarcimento del danno.

Altrettanto adattabile alla fattispecie degli *smart contract* è sia la predisposizione di una clausola risolutiva espressa (art. 1456 cod. civ.) che consenta la risoluzione di diritto del contratto non appena il sistema accerti che le modalità stabilite per l'adempimento di una determinata obbligazione non siano rispettate; sia l'apposizione di un termine essenziale (art. 1457 cod. civ.) alla scadenza del quale lo *smart contract* può consentire alla richiesta anche tardiva di esecuzione (art. 1457, comma 1) o alla risoluzione del contratto in seguito al perdurare dell'inadempimento (art. 1457, comma 2).

La risoluzione del contratto ha effetto retroattivo tra le parti, “salvo il caso di contratti ad esecuzione continuata o periodica, riguardo ai quali l'effetto della risoluzione non si estende alle prestazioni già eseguite” (art. 1458 cod. civ.). La risoluzione non pregiudica la posizione dei terzi, anzi vi è “la possibilità che lo *smart contract* riceva l'informazione dell'avvenuta trascrizione di risoluzione e ne tenga conto, appunto, per quei diritti dei terzi che, poiché derivati dallo *smart contract*, questo possa continuare a controllare, dando ad essi terzi notizia diretta dell'avvenuta trascrizione e, in uno scenario di evoluzione del sistema, condizionarne direttamente l'esecuzione una volta che la domanda di risoluzione sia stata decisa”¹³⁹.

¹³⁸ Non può essere ovviamente prefigurata dallo *smart contract* la fattispecie per cui si può recedere dal contratto qualora controparte “non abbia un interesse apprezzabile all'adempimento parziale” (art. 1464 cod. civ.). In questo caso, infatti, bisognerebbe immaginare la figura di un terzo che guidi lo *smart contract* nell'individuazione di ciò che sia o meno “apprezzabile”.

¹³⁹ GENTILE, *Vicende patologiche del contratto in forma di smart contract*, in AA.VV., *Blockchain e smart contract*, cit., 337.



13. – Un altro rimedio ad una situazione patologica è l'azione di rescissione, ammessa dal nostro legislatore qualora il contratto sia stato concluso in stato di pericolo (art. 1447 cod. civ.) o con sproporzione tra le prestazioni che sia dipesa dallo stato di bisogno di una delle parti contraenti (art. 1448 cod. civ.)¹⁴⁰. Avuto riguardo alla natura dello *smart contract*, certamente non è prospettabile la prima fattispecie di rescissione perché il dialogo tra computer con la conseguente apposizione di firma o codici identificativi a sancirne la validità non può essere subordinato al riconoscimento di uno *status* soggettivo di pericolo. Né sembra ipotizzabile che nel codice dello *smart contract* le parti possano indicare ogni variabile immaginabile di situazione di pericolo con una *library* infinita di opzioni.

Compatibile è, invece, per certi versi, l'ipotesi di rescissione del contratto concluso in stato di bisogno. Le funzioni dello *smart contract*, infatti, ben potrebbero essere attivate per riconoscere la lesione *ultra dimidium* che essendo elemento misurabile, una volta calcolato, potrebbe attivare una funzione che rescinda il contratto. Il sistema, al quale è inviata la domanda di rescissione, può evitarla proponendo una modifica del contratto tale da ricondurlo ad equità (art. 1450 cod. civ.). Ma poiché indici valoriali, quali l'equità (ma anche la buona fede, la correttezza, la colpa etc.), non sono calcolabili dallo *smart contract*, le parti possono ovviare a questo impasse, predeterminando il giusto prezzo che deve essere corrisposto a fronte di una determinata prestazione. Superato il termine di un anno dalla conclusione del contratto, la funzione rescissione si disattiva, ferma comunque la possibilità di riattivarla nel caso in cui ci si trovi dinanzi ad una fattispecie di reato, nel qual caso il termine di prescrizione sarà diverso¹⁴¹ (art. 1449 cod. civ.).

14. – Seppure i sostenitori della blockchain ritengano gli *smart contract* infallibili e, perciò, insuscettibili di far sorgere controversie tra le parti nel momento della loro esecuzione¹⁴² o, comunque, in grado di autoregolarsi e di assicurare alle parti giustizia sostanziale, questa affermazione non sembra del tutto convincente. È più realistico pensare che tra le parti possano sorgere conflitti che debbano trovare opportuna risoluzione nel mondo reale ad opera delle giurisdizioni competenti¹⁴³. Ai fini della individuazione della legge applicabile è preliminare ricordare che raramente gli *smart contract* si sviluppano a seguito dell'impiego di nodi localizzati in un solo Stato (o che, comunque, siano coordinati da una entità territorialmente ben individuata)¹⁴⁴, ma che, più spesso, essi sono gestiti in modo decentrato dai membri della rete. La tecnologia blockchain è nata, infatti, per funzionare indipendentemente da centri di imputazione o di interesse (o dai luoghi dei singoli computer¹⁴⁵) e consente di sottoscrivere contratti transnazionali che, proprio in quanto registrati su un registro distribuito, sono delocalizzati ed operano al di fuori di un preciso quadro normativo¹⁴⁶. I soggetti (per-

¹⁴⁰ D. LORUSSO, N. GENTILE, *Blockchain e annullamento contrattuale. Spunti di discussione*, in <https://www.blblex.it/blog>.

¹⁴¹ Anche in questo caso teoricamente lo *smart contract* potrà essere programmato, e quindi il termine di prescrizione modificato, una volta che il sistema abbia individuato il reato.

¹⁴² F. MOSLEIN, *Conflicts of laws and codes: defining the boundaries of digital jurisdiction*, in <https://ssrn.com/abstract>; V. ZAMFIR, *Against Szabo's law. For a new crypto legal system*, in <https://medium.com>.

¹⁴³ CARNELUTTI, *Teoria generale del diritto*, Roma, 1940, 14, secondo cui in ogni fenomeno giuridico sarebbe rintracciabile *in nuce* un conflitto e, di conseguenza, il diritto esiste in quanto vi è un conflitto.

¹⁴⁴ M. FINCK, *Blockchain Regulation and Governance in Europe*, Cambridge, 2018, 19.

¹⁴⁵ N. IRTI, *Norme e luoghi. Problemi di geo diritto*, Roma-Bari, 2006, 65, secondo cui “la globalizzazione nella rete telematica raggiunge il suo grado più elevato” e ... “nello spazio telematico non sono certo individuabili i luoghi dei singoli computer”, piuttosto la rete telematica è “un non luogo, poiché i luoghi appartengono a terra, mare, aria”.

¹⁴⁶ Più volte è dovuta intervenire la Corte di Giustizia pronunciandosi sulle condotte antiggiuridiche tenute da alcune big-tech nello spazio giuridico europeo e rese possibili dallo sfruttamento di c.d. vuoti normativi (Corte di giustizia, 24 settembre 2019, in causa C-



sono fisiche o giuridiche) che intendono valersi della blockchain in ambito nazionale devono verificare e rispettare le norme del proprio paese di origine, ma ove la contrattazione avvenga con membri della rete allocati in stati diversi, la situazione, salvo accordo tra le parti, rende impossibile l'individuazione di un ordinamento nazionale cui fare riferimento. Di là dalla prospettazione di una *lex cryptographica*¹⁴⁷ o di una *lex informatica*¹⁴⁸ agognata dagli sviluppatori e dai membri della rete, è ragionevole chiedersi se, in questi casi, possa soccorrere la disciplina uniforme europea ed in particolare il Regolamento Bruxelles I bis¹⁴⁹ ed il Regolamento Roma I¹⁵⁰, con riferimento alle questioni di giurisdizione e di legge applicabile alle obbligazioni contrattuali in materia civile e commerciale. Certamente i Regolamenti richiamati, nella loro versione attuale, non sembrano adattabili alla contrattazione che si sviluppi a mezzo di *smart contract* perché concepiti per risolvere il conflitto di leggi nel mondo fisico. Sarebbero, pertanto, necessarie talune modifiche *ad hoc* in considerazione della peculiare natura della tecnologia utilizzata. In particolare, di là dalle modifiche che dovrebbero coinvolgere i fori speciali¹⁵¹, con riguardo al foro generale di cui all'art. 4 del regolamento Bruxelles I bis¹⁵², sarebbe necessario l'introduzione di un ulteriore titolo di giurisdizione generale, sussidiario al

507/17, *Google LLC c. Commission nationale de l'informatique et des libertés (CNIL)*; Corte di giustizia, 24 settembre 2019, in causa C-136/17, *GC et al c. Commission nationale de l'informatique et des libertés (CNIL)*; Corte di giustizia, 28 gennaio 2019, in causa C-567/19, *Coty Germanu G, bH c. Amazon Services Europe Sàrl*; Corte di giustizia, 20 dicembre 2017, in causa C-343/15, *Asociación Profesional Elite Taxi c. Uber Systems Spain*; Corte di giustizia, 28 luglio 2016, in causa C-191/15, *Verein für Konsumenteninformation c. Amazon EU Sarl*. Tutte le sentenze sono rintracciabili in <https://curia.europa.eu/juris/>.

¹⁴⁷ Alcuni autori, proponendo un interessante parallelismo con la *lex mercatoria*, hanno suggerito la creazione di una *lex cryptographica* che debba disciplinare l'utilizzo e lo scambio di informazioni digitali in modo da promuovere la stabilità e la prevedibilità delle regole del mondo virtuale. Il meccanismo di regolamentazione basato su numeri ed algoritmi dovrebbe essere incorporato direttamente nel tessuto del sistema tecnologico e si caratterizzerebbe, oltre che per la capacità di dettare dei vincoli e fornire degli incentivi per i membri della comunità, anche per il fatto di operare in modo autonomo, indipendentemente da qualsiasi governo o da altra autorità centralizzata (T. ORSOLA, *The lex mercatoria in theory and practice*, Oxford, 2017; A. WRIGHT, P. DE FILIPPI, *Decentralized blockchain technology and the rise of lex cryptographa*, in <https://ssrn.com/abstract>; L. LESSIG, *The laws of cyberspace*, United States, 1998).

¹⁴⁸ R. REIDENBERG, *Lex informatica. The formulation of information policy rules through technology*, in *Texas law review*, 2020, 553. Si tratterebbe, secondo l'autore di un insieme di regole interne alla rete, sviluppate attraverso soluzioni tecnologiche, disancorate dalle norme statuali e, quindi, di facile attuazione mediante il controllo dello strumento tecnico.

¹⁴⁹ Regolamento (UE) n. 1215/2012 del Parlamento europeo e del Consiglio del 12 dicembre 2012 concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale, in *G.U.U.E.* L351/1 del 20 dicembre 2012.

¹⁵⁰ Regolamento (CE) n. 593/2008 del Parlamento europeo e del Consiglio, del 17 giugno 2008, sulla legge applicabile alle obbligazioni contrattuali (Roma I), in *G.U.U.E.* L177/6 del 4 luglio 2008.

¹⁵¹ Anche con riguardo ai fori speciali, la dottrina ha proposto ulteriori modifiche. In particolare, con riferimento al foro di cui al contratto di compravendita (art. 7.1 b) il legislatore dovrebbe prevedere che, in ipotesi di compravendita di *token*, il luogo di consegna debba coincidere con il luogo ove vi è stata l'apprensione fisica del bene (rappresentato dal *token*) ovvero ove l'acquirente è stato messo nella possibilità di liberamente disporre del bene immateriale. Tale criterio avrebbe l'ulteriore conseguenza di privare di effetti reali il trasferimento del *token* "posticipando" l'evento-esecuzione della prestazione caratteristica del rapporto (ossia la consegna del bene) al momento in cui l'acquirente può effettivamente utilizzarlo. L'intervento del legislatore dovrebbe altresì riguardare le obbligazioni extracontrattuali (art. 7.2). Qualora l'illecito extra contrattuale sia stato prodotto su *blockchain*, la parte danneggiata dovrebbe poter scegliere di instaurare la controversia avanti il giudice del luogo ove risiede. La giurisdizione rimarrebbe così strettamente correlata, favorendola, alla parte più debole del rapporto, indipendentemente dal luogo dove la condotta è stata tenuta o il danno si è verificato o può avvenire. Questi ultimi sarebbero infatti pressoché impossibili da reperire. Correlativamente, il ricorso a una previsione *de jure condendo* si impone anche qualora si debba ricorrere ai c.d. fori speciali di protezione (cfr. artt. 10, 17 et 19 Reg. Bruxelles I bis). In proposito, si ritiene quanto mai opportuno che il legislatore europeo intervenga sulla disciplina sostanziale di ciascuna tipologia contrattuale (assicurazioni, consumatori, lavoratori) prevedendo che, quando negoziate in uno *smart legal contract*, pongano come condizione necessaria di validità la individuazione del luogo di domicilio delle parti coinvolte, chiarendo peraltro quella che agisce in qualità di, rispettivamente, assicurato, consumatore e lavoratore.

¹⁵² L'art. 4 1. Stabilisce che "a norma del presente regolamento, le persone domiciliate nel territorio di un determinato Stato



domicilio del convenuto spesso difficile (se non impossibile) da reperire. Nello specifico potrebbe autorizzarsi l'attore ad instaurare il procedimento avanti al giudice del foro ove si trova l'indirizzo fisico in cui il convenuto ha dato il proprio consenso alla "costruzione" dello *smart contract*. Ciò, indipendentemente da come l'ordinamento giuridico del Paese ove si trova tale indirizzo lo qualificherebbe (domicilio, residenza, dimora). Tecnicamente, si tratta, peraltro, di una individuazione facile purché gli sviluppatori della blockchain inseriscano il comando che rende possibile la registrazione della provenienza "fisica" dell'ordine¹⁵³.

Anche il Regolamento Roma I sulla legge applicabile alle obbligazioni contrattuali necessiterebbe di alcune modifiche con riferimento al criterio principale di collegamento. In particolare, con riferimento all'art. 3.1¹⁵⁴, il legislatore potrebbe legittimare la *optio legis*, circa la scelta fatta dalle parti sulla legge applicabile, quando esercitata nel rispetto di una determinata procedura. La scelta di legge andrebbe effettuata nel contratto da eseguire nel mondo virtuale oppure in un accordo separato dallo *smart contract* e concluso fra le parti. Le parti potrebbero persino concordare una specifica funzione dello *smart contract* che, se eseguita, sussuma il rapporto *inter partes* all'interno di un determinato quadro normativo (ad esempio con la dicitura "questo contratto è stato interpretato in conformità e regolato dalla legge (...)")¹⁵⁵. La scelta, a norma dell'art. 3.1 del Regolamento Roma I può avvenire anche in modo implicito ove essa risulti chiaramente dalle disposizioni del contratto o dalle circostanze del caso. Si pensi, ad esempio, alla circostanza in cui nello *smart contract* ci si riferisse ad un particolare sistema giuridico, ciò farebbe presumere che le parti avrebbero scelto la legge di tale sistema giuridico per regolare il rapporto contrattuale.

In considerazione di quanto rilevato è ragionevole ipotizzare che se, nella pratica, le parti dello *smart contract* non hanno determinato la legge del contratto e non sia applicabile la disciplina di diritto uniforme, le controversie insorte possono essere risolte da un arbitro ai sensi dell'art. 806 c.p.c. Le parti possono stipulare un compromesso quando già la lite è insorta tra loro (art. 807 c.p.c.), oppure possono convenire una clausola arbitrale (art. 808 c.p.c.) inserendola nello *smart contract* o in altro documento (cartaceo o informatico) che, però, faccia espresso riferimento alle controversie sorte da quel rapporto negoziale. Le parti possono, peraltro, optare per un arbitrato da celebrarsi *on chain* (su catena)¹⁵⁶. Il lodo viene registrato nel mondo virtuale

membro sono convenute, a prescindere dalla loro cittadinanza, davanti alle autorità giurisdizionali di tale Stato membro. Alle persone che non possiedono la cittadinanza dello Stato membro nel quale esse sono domiciliate si applicano le norme sulla competenza vigenti per i cittadini di tale Stato membro".

¹⁵³ Sul punto si veda B. CAPPIELLO, Dallo "*smart contract*" computer code allo *smart (legal) contract*. *I nuovi strumenti (para) giuridici alla luce della normativa nazionale e del diritto internazionale privato europeo: prospettive de jure condendo*, in *Dir. comm. int.*, 2020, 2, 477.

¹⁵⁴ L'articolo 3.1 in tema di libertà di scelta statuisce che "Il contratto è disciplinato dalla legge scelta dalle parti. La scelta è espressa o risulta chiaramente dalle disposizioni del contratto o dalle circostanze del caso. Le parti possono designare la legge applicabile a tutto il contratto ovvero a una parte soltanto di esso".

¹⁵⁵ B. CAPPIELLO, Dallo "*smart contract*" computer code allo *smart (legal) contract*. *I nuovi strumenti (para) giuridici alla luce della normativa nazionale e del diritto internazionale privato europeo: prospettive de jure condendo*, cit., 480. Per quanto concerne i criteri di collegamento speciali, l'autore suggerisce che il primo cui apportare una modifica sia quello di cui "all'art. 4.1 ossia quello della residenza abituale. Posta la difficoltà di reperire tale luogo, il legislatore potrebbe aggiungere un criterio alternativo da applicare in ipotesi di *smart legal contract*. Si potrebbe dunque rinviare alla legge del luogo ove la parte che esegue la prestazione caratteristica ha prestato il proprio consenso. Non si ravvisa invece la possibilità né di impiegare né di modificare il criterio residuale del collegamento più stretto di cui all'art. 4.4; come visto, si tratta invero di un luogo pressoché impossibile da individuare quando si impiega tecnologia a registro distribuito. In tutti i citati casi, però, nelle more di un intervento normativo e nell'impossibilità di applicare la disciplina europea uniforme attualmente in vigore, la controversia sarà risolta ricorrendo al diritto internazionale processuale nazionale".

¹⁵⁶ In tal senso si pensi alla proposta di *Jur* (in <https://jur.io>). Si tratta sostanzialmente di una tradizionale procedura arbitrale sulla



ed “eseguito sulla stessa blockchain, tramite l’esecuzione di un codice che preveda il trasferimento delle somme riconosciute come dovute dal lodo arbitrale dal conto riconducibile alla parte condannata a quello riconducibile alla parte vincitrice”¹⁵⁷.

15. – Alla luce di quanto detto può affermarsi che lo *smart contract* è, al contempo, il mezzo attraverso il quale l’accordo si manifesta e lo “strumento grazie al quale esso può concludersi”¹⁵⁸. Lo *smart contract*, in quanto programma informatico che non ha una propria capacità decisionale ma attua semplicemente una volontà altrui (programmata e vincolante) non può essere assimilato ad un soggetto giuridico né è prefigurabile la sua riconduzione alla fattispecie rappresentativa¹⁵⁹.

Alla luce di tali premesse e, considerato che il d.lgs. n. 70 del 9 aprile 2003¹⁶⁰ prevede che “le norme sulla conclusione dei contratti si applicano anche nei casi in cui il destinatario di un bene o di un servizio della società dell’informazione inoltri il proprio ordine per via telematica” (art. 13, comma 1), sul piano della disciplina, non può negarsi la compatibilità tra contratti telematici e contratti non virtuali¹⁶¹. L’estensione delle norme sulla conclusione dei contratti anche ai contratti telematici, senza che si preveda allo stato un’adeguata disciplina di dettaglio, consente di ritenere che la contrattazione telematica richiede un flessibile adattamento delle norme di diritto interno ai nuovi procedimenti di formazione e conclusione dei contratti¹⁶². In questa direzione appare plausibile il tentativo di recupero delle tradizionali categorie civilistiche per governare le questioni che gli *smart contract* pongono e per prevenire i conflitti che possano eventualmente sorgere a seguito del loro utilizzo¹⁶³. In previsione dei nuovi sviluppi della tecnologia, ove le fonti applicabili dovessero risultare carenti, il procedimento di inclusione dei nuovi strumenti potrebbe richiedere l’intervento del legislatore. Infatti, seppure il modello del registro distribuito e gli *smart contract* nascano come

blockchain progettata per controversie complesse e di medio/alto valore, nella quale gli *Admins* (ovvero Istituzioni arbitrali o studi legali) possono creare i c.d. “*Arbitration Hubs*”, equivalenti alle camere arbitrali. L’*Admin* prima di tutto deve predisporre un regolamento arbitrale conforme alle norme internazionale (come ad esempio la Convenzione di New York) e individuare gli arbitri. Infine, l’*Admin* determina il valore massimo delle controversie che l’*Arbitration Hub* può trattare. Quando le parti convengono di fare decidere la controversia alla camera arbitrale X (*Arbitration Hub*) viene individuato un arbitro che gestirà un procedimento online basato sulla tecnologia *blockchain* nella quale, ad esempio, vengono salvate le prove (per evitare che vengano modificate); alla fine del procedimento l’arbitro dovrà redigere una bozza di lodo che verrà sottoposta a un sistema di *peer-review*, ovvero la bozza prima di diventare definitiva viene inviata a tre arbitri di un altro *Arbitration Hub*: se supera questo sistema di revisione allora il lodo diventa definitivo, altrimenti viene nominato un nuovo arbitro. L’arbitro guadagna e/o perde “punti di reputazione” in base a questo sistema di *peer-review* (R. BATTAGLINI, *La tecnologia blockchain e le nuove forme della Dispute Resolution*, intervento al Convegno sul tema “La risoluzione dei conflitti nell’era digitale: L’arbitrato e la rivoluzione tecnologica”, Milano, 21 novembre 2019).

¹⁵⁷ C. PONCIBÒ, *Smart contract: profili di legge applicabile e scelta del foro*, in AA.VV., *Blockchain e smart contract*, cit., 370.

¹⁵⁸ M. PENNASILICO, *La conclusione dei contratti online tra continuità e innovazione*, in *Diritto dell’informatica*, 2004, 6, 805.

¹⁵⁹ In dottrina sulla c.d. rappresentanza elettronica G. SARTOR, *Gli agenti software: nuovi soggetti del ciberdiritto?*, in *Contratto e impresa*, 2002, 485; ID., *Gli agenti software e la disciplina giuridica degli strumenti cognitivi*, in *Dir. inf. e informatica* 2003, 77. Contra DI G. ROSA, *Quali regole per i sistemi automatizzati intelligenti?*, in *Riv. dir. civ.*, 2021, 843, secondo cui l’individuazione in capo allo *smart contract* di un potere rappresentativo non produrrebbe alcuna semplificazione del sistema giuridico anzi determinerebbe ancora maggiori incertezze rispetto ad alcune questioni classiche in tema di rappresentanza (vizi del consenso e stati soggettivi rilevanti, mezzi idonei ad assicurare pubblicità alla procura, falsa rappresentanza e rappresentanza senza poteri, etc.).

¹⁶⁰ D.lgs. n. 70 del 9 aprile 2003, n. 70 (Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell’informazione nel mercato interno, con particolare riferimento al commercio elettronico), cit.

¹⁶¹ R. TORINO, *I contratti finanziari conclusi tramite internet*, in AA.VV., *I contratti del mercato finanziario*, Torino, 2004, I, 479.

¹⁶² M. PENNASILICO, *La conclusione dei contratti online tra continuità e innovazione*, cit., 805.

¹⁶³ G. FINOCCHIARO, *Il contratto nell’era dell’intelligenza artificiale*, in *Rivista trim. dir. proc. civ.*, 2018, 2, 441.



reazione al potere delle autorità centrali, come “manifesto di una nuova cripto anarchia”¹⁶⁴, gli ordinamenti nazionali devono porsi come presidio avanzato di governo della rivoluzione tecnologica¹⁶⁵. A livello strategico, in Italia nel dicembre 2018 è stato nominato dal Ministero dello Sviluppo Economico un gruppo di esperti provenienti da diversi contesti di riferimento (imprese, associazioni di categoria, università, ricerca, Pubblica Amministrazione, società civile, organizzazioni sindacali, terzo settore e associazioni dei consumatori) con l’obiettivo di individuare proprie iniziative, *use cases* abilitanti e buone prassi esistenti, elaborare strumenti per creare e favorire condizioni economiche, politiche e regolatorie, individuare gli strumenti tecnici e normativi volti a diffondere l’applicazione degli *smart contracts* e fornire indirizzi strategici e modelli di *governance*. E l’inizio di un percorso che verosimilmente potrà (o dovrà) condurre, innanzitutto, alla elaborazione di specifiche previsioni volte a ridurre il divario digitale fra chi è perfettamente inserito tecnologicamente e chi è escluso dalla catena e dal flusso di dati¹⁶⁶. La potenza elaborativa delle macchine se, infatti, per un verso favorisce l’iniziativa economica privata (art. 41 della Costituzione), per altro crea forti dicotomie sociali derivanti, più che dall’accesso alla rete, dall’uso che viene fatto della stessa¹⁶⁷. È quindi importante stimolare un percorso di trasformazione finalizzata alla educazione ed alla cultura digitale senza le quali, nella società dell’informazione, nell’era dei robot, degli algoritmi e dei *big data* non potrà risultare rispettato il principio di uguaglianza tra i contraenti e della tutela dei contraenti deboli¹⁶⁸.

Non meno importante, è la predisposizione di un diritto il quale, seppure flessibile in considerazione dei nuovi contenuti e della mutata terminologia giuridica¹⁶⁹, possa aprire ulteriori spazi per l’utilizzo degli *smart contract* in campi diversi dal dominio del *finance*. *De iure condendo*, infatti, potrebbe considerarsi l’ipotesi di sfruttare le nuove tecnologie, una volta che si siano sufficientemente stabilizzate, per costituire garanzie (*smart guarantees*) o per redigere testamenti (*smart will*). La rilevanza giuridica e lo sviluppo dello *smart contract* sono certamente destinati a rivoluzionare il diritto del terzo millennio.

¹⁶⁴ S. CAPACCIOLI, *Smart contracts: traiettoria di un’utopia divenuta attuabile*, Modena, 2016, 26.

¹⁶⁵ S. CERRATO, *Contratti tradizionali, diritto dei contratti e smart contract*, in AA.VV., *Blockchain e smart contract*, cit., 312.

¹⁶⁶ Il fenomeno noto con il nome di “*digital divide*” (divario digitale) è il divario esistente tra chi ha accesso effettivo alle tecnologie dell’informazione (in particolare personal computer e Internet) e chi ne è escluso, in modo parziale o totale. I motivi di esclusione comprendono diverse variabili: condizioni economiche, livello d’istruzione, qualità delle infrastrutture, differenze di età o di sesso, appartenenza a diversi gruppi etnici, provenienza geografica. Oltre a indicare il divario nell’accesso reale alle tecnologie, la definizione include anche disparità nell’acquisizione di risorse o capacità necessarie a partecipare alla società dell’informazione: nei paesi avanzati, e specie nella popolazione giovane, infatti, il divario di mero accesso alla rete è ormai quasi del tutto colmato e si apre invece un divario digitale di secondo livello basato sulle modalità di fruizione. Il termine *digital divide* può essere utilizzato sia per riferirsi ad un divario esistente tra diverse persone, o gruppi sociali in una stessa area, che al divario esistente tra diverse regioni di uno stesso stato, o tra stati (o regioni del mondo) a livello globale.

¹⁶⁷ L. ATTIAS, M. MELCHIONDA M. PIACITELLI, A. RUGGIERO, *Mind the gap!*, in *Rivista elettronica di diritto, economia, management*, 2017, 3, 94.

¹⁶⁸ L. ATTIAS, G. SCORZA, *La consapevolezza digitale al servizio dell’etica*, in *Diritto inf. e dell’informatica*, 2019, 6, 1191.

¹⁶⁹ AMATO, A. MANGIAMELI, *Tecno-regolazione e diritto. Brevi note su limiti e differenze*, in *Dir. inf. e dell’informatica*, 2017, 2, 147.