

Massimo Giuliano

**LA BLOCKCHAIN E GLI
SMART CONTRACTS
NELL'INNOVAZIONE DEL DIRITTO
NEL TERZO MILLENNIO**

Estratto



GIUFFRÈ FRANCIS LEFEBVRE

MASSIMO GIULIANO

LA BLOCKCHAIN E GLI *SMART CONTRACTS* NELL'INNOVAZIONE DEL DIRITTO NEL TERZO MILLENIO

SOMMARIO: 1. Il ruolo del giurista nell'era della tecnologia blockchain. — 2. I *Distributed Ledger Technologies*. Dalla blockchain pubblica dei Bitcoin alle blockchain private: profili tecnologici. — 2.1. *Segue*. La crittografia in uso nella Blockchain Bitcoin. — 2.2. *Segue*. La funzione hash. — 2.3. *Segue*. Le blockchain *permissionless*, *permissioned* e del tipo *consortium*. — 3. Le questioni giuridiche: la tecnologia blockchain e la protezione dei dati personali alla luce del Regolamento europeo 2016/679. — 3.1. *Segue*. Il profilo dell'identità degli individui nel mondo virtuale e l'imputazione della volontà. — 4. Dal contratto cibernetico allo *smart contract*. — 4.1. La natura giuridica dello *smart contract*. — 4.2. La forma dello *smart contract*. — 4.3. La manifestazione del consenso nell'automazione contrattuale e i criteri di imputazione della volontà. — 5. Conclusione.

1. IL RUOLO DEL GIURISTA NELL'ERA DELLA TECNOLOGIA BLOCKCHAIN.

La tecnologia ha da sempre influito sul modo in cui i consociati regolano le proprie relazioni e, quindi, indirettamente, sul diritto che governa la società¹. L'avvento della tecnologia blockchain, definita “disruptive”², sta generando un mutamento delle relazioni umane, che, gioco forza, influiscono sul diritto, in special modo sulla sua funzione di strumento di tutela e di soluzione dei conflitti. Sorge l'esigenza di proteggere tutte quelle proiezioni della persona all'interno del mondo virtuale, cui il soggetto accede attraverso una identità digitale, così definita poiché costituisce la rappresentazione virtuale di una identità di una persona che la utilizza come mezzo di connessione tra il reale e il digitale. Con lo sviluppo di Internet si è passati da una funzione passiva³, dove gli

¹ G. PASCUZZI, *Il diritto dell'era digitale*, Bologna, 2002, 61-66, dove l'Autore pone in evidenza il fatto che la tecnologia da un lato determina il verificarsi di nuove situazioni che possono minare la riservatezza degli individui, dall'altro predispone anche dei rimedi da utilizzare per la difesa dei propri dati personali.

² Così definita poiché “bring to a market a very different value proposition than had been available previously”, in questo senso BOWER-CHRISTENSEN, *Disrupting Technologies: Catching the Wave*, in *Harvard Business Review*, I, 1995, 10.

³ Internet nasce come ARPANet (dal nome dell'agenzia di ricerca americana che

utenti erano limitati alla visione di informazioni che venivano fornite loro, ad un modello di utilizzo che prevede una crescente interazione con la rete, applicazioni *web* interattive che facilitano la condivisione delle informazioni, l'interoperabilità e la collaborazione nel *World Wide Web*⁴, come, ad esempio, i processi di registrazione ed utilizzo dei *social network* o delle piattaforme che erogano i più svariati servizi dove ciascun utente inserisce i propri dati a fronte del rilascio di credenziali di accesso (ad esempio *user id* e *password*), che altro non sono se non la rappresentazione biunivoca tra l'utente e i suoi attribuiti identificativi⁵. L'identità digitale, tuttavia, è il frutto anche di un processo continuo che la arricchisce di un patrimonio informativo formato "non solo su ciò che è e fa chi ne dispone, ma anche sulle relazioni e reazioni che i suoi atti sono in grado di generare"⁶. L'identità digitale, pertanto, può assumere diverse forme che, non necessariamente, ma spesso, si allontanano dall'identità personale del soggetto, sia per il tramite di informazioni che altri elaborano sullo stesso, sia per la veridicità di informazioni che lo stesso soggetto comunica alla rete. È pur vero che vi sono dei servizi *on line* che per poter essere fruiti necessitano di informazioni vere e precise sull'identità personale di un soggetto e certificate da altri soggetti a tale scopo autorizzati, come si avrà modo di vedere nel prosieguo.

Il giurista, dunque, non può trascurare tale fenomeno sociale, poiché il diritto è esso stesso fenomeno sociale⁷, che muta nel corso del tempo in quanto "prodotto e contemporaneamente motore di cambiamenti culturali, economici, sociali e politici". Lo studioso di diritto, al contrario di studiosi di altre scienze, deve

l'aveva progettata, *Advanced Research Project Agency*) nel 1969 con l'obiettivo di realizzare un flessibile strumento di comunicazione adatto a garantire il collegamento tra strutture militari, anche in caso di interruzioni delle linee principali di comunicazione (V. A. APARO, *Il libro delle reti*, Roma, 1995).

⁴ La data di nascita del *World Wide Web* viene comunemente indicata nel 6 agosto 1991, giorno in cui l'informatico inglese Tim Berners-Lee pubblicò il primo sito web. È il sistema di comunicazione più impiegato, tanto da diventare sinonimo di Internet. Il *www* utilizza un linguaggio denominato HTML (Hyper Text Mark-up Language) sviluppato dal CERN di Ginevra per consentire ai gruppi di ricercatori ed ingegneri diffusi nelle più svariate parti del mondo la condivisione *on line* di dati rilevanti per le loro ricerche.

⁵ ROVEGNO Angelo Osvaldo, *Identità digitale: tra esigenze di condivisione e necessità di tutela*, in *Cyberspazio e Diritto* 2013 fasc. 3, pp. 403-423.

⁶ V. GIGLIO, *Identità e profilazione digitale: i rischi dei Big Data*, in *FiLO diritto*, 22 novembre 2016, pp. 1-8.

⁷ G. PASCUZZI, *La creatività del giurista*, Bologna, 2013, p. 2. Arnold Roosenale identifica il concetto di persona digitale in tre forme diverse: una forma *Progettata*, una *Imposta* ed una *Ibrida*. La forma progettata è quella che l'individuo sceglie, forma e rappresenta per mezzo dei contenuti che immette, come ad esempio nel caso di una homepage di un sito personale; la forma imposta è l'identità creata da enti esterni, attraverso le elaborazioni di dati che ci riguardano, come nel caso della determinazione del merito creditizio da parte delle società di rating; la forma ibrida è la rappresentazione creata dal web 2.0 e dalle sue connessioni sociali, specialmente attraverso la profilazione dei dati raccolti nei siti che si visitano o ai quali ci si registra, come nel caso dei *social network*. In questo senso A. ROOSENALE, *Digital personae and profiles as representations of individuals*, in *Pri-*

vivere intensissimamente la vita che si srotola e rotola sotto i suoi occhi osservando i fenomeni sociali che agitano il mondo siano essi politici, artistici, religiosi⁸. Nella ricerca dei mezzi di tutela da apprestare alle molteplici e complesse istanze che l'individuo nella sua dimensione digitale avanza⁹, il giurista deve aprirsi al cambiamento e contribuire alla creazione della nuova cornice regolamentare in ragione dello strumentario giuridico esistente e, ove necessario, sollecitare l'intervento del legislatore affinché elabori soluzioni nuove che siano al passo con la tecnologia e che allo stesso tempo non la ingessino entro gli angusti limiti di una regola settoriale.

La tecnologia dell'informazione ha trasformato il modo in cui le aziende operano. Essa consente alle aziende di automatizzare operazioni manuali e processare l'informazione più in fretta. Internet ha creato nuove forme di comunicazione e altri metodi di lavoro che le imprese utilizzano durante l'elaborazione delle informazioni finanziarie e di *business*. In questo epocale cambiamento vi è chi ha avuto modo di osservare che il mercato, luogo ideale entro il quale avvengono, tendenzialmente in autonomia, gli scambi tra le parti, non è una realtà autonoma, ma è prodotto dell'ordinamento giuridico, non potendo esistere, né potendo gli individui operare in esso, senza regole giuridiche che lo ordinino¹⁰.

Il mercato ha regole proprie, imposte proprio dalla nascita di nuovi modelli di *business* prima inimmaginabili, di cui l'ordinamento non può non tenere conto. È innegabile la difficoltà di regolare *ex ante* e in astratto fenomeni innovativi dirompenti, come è stato Internet 30 anni fa e come è adesso la tecnologia blockchain e le sue applicazioni nelle relazioni sociali. E “questo è tanto più necessario in quanto l'innovazione scientifica e tecnologica si fa portatrice di un mutamento incessante che non può essere governato attraverso il tradizionale inseguimento legislativo. È indispensabile, quindi, “privilegiare strumenti “prospettici”, quali sono appunto quelli legati a una normativa per principi, mentre la costruzione di una disciplina affidata a fattispecie chiuse presuppone un diritto che interviene alla fine di un ciclo, che scende alla sera, per selezionare e razionalizzare interessi e situazioni ormai consolidati”¹¹. Purtroppo, il diritto può scegliere — in considerazione dello specifico settore in cui deve essere applicato — la via delle *sunset rules*, delle norme destinate a

vacy and identity management for life, 2010, *passim*.

⁸ In questo senso S. SATTA, *Colloqui e soliloqui di un giurista*, Padova, 1967, p. XIX.

⁹ Prima tra tutte la tutela della propria identità digitale.

¹⁰ Così A. CATAUDELLA, *L'uso abusivo di principi*, in *Riv. dir. civ.*, 2014, 4, p. 747.

¹¹ S. RODOTÀ, *Tecnopolitica, la democrazia e le nuove tecnologie della comunicazione*, Roma-Bari 2004.

tramontare e ad essere sostituite ad una scadenza predeterminata, prevedendo così un obbligo del legislatore (o di altri soggetti) di riconsiderare la materia ¹².

Appare, peraltro, di notevole interesse in tale contesto il dialogo tra due illustri studiosi, Natalino Irti ed Emanuele Severino ¹³, in ordine al rapporto tra diritto e tecnica, nella duplice ottica del giurista e del filosofo, dal quale emerge da un lato — nella visione del giurista — la concezione positivistica del diritto, fatto di norme aventi esclusivamente validità procedurale, e non verità di contenuto, in cui è all'interno di tali norme che le proposizioni ideologico-politiche o economiche devono tradursi per riuscire ad ottenere efficacia. La stessa tecnica, sostiene Irti, sarebbe segnata dalla medesima astrattezza e perciò non in grado di rispondere alle domande fondamentali del diritto. Dall'altro lato, nella visione del filosofo, la tecnica è, invece, “destinata a diventare il principio regolatore di ogni materia, la volontà che regola ogni altra volontà”. Severino, partendo dall'idea di fondo che la tecnica, per sua essenza, non mira a scopi escludenti, bensì ha come scopo la crescita infinita nella propria potenza, giunge ad affermare che essa stessa rivela una sua concretezza, poiché è la forma della produzione reale degli scopi, produzione che concorre all'aumento indefinito dell'apparato scientifico-tecnologico. Irti, tuttavia, a suo giudizio ritiene che la tecnica, in quanto “forma di volontà mirante per raggiungere scopi non escludenti, escluderebbe tutti gli scopi contrastanti con la propria infinita capacità di raggiungere scopi”.

Contestualizzando il dialogo tra i due illustri Autori nel contesto in cui la nostra analisi si colloca, non credo che il diritto debba piegarsi alla tecnica lasciando che questa imponga la regolazione, ma, al contrario appare necessario che le nuove tecnologie passino sotto lo scrutinio del giurista affinché egli possa plasmare il diritto esistente al nuovo che avanza, nel rispetto dei principi di ciascun ordinamento nel quale il fenomeno è analizzato. Laddove lo strumentario giuridico si riveli inefficace a disciplinare nuove forme di relazioni, specie laddove ci si trovi di fronte a paradigmi del tutto nuovi, come nel caso dei rapporti dematerializzati eseguiti in una rete senza intermediari, dove, oltre ai beni, è la stessa persona ad assumere un'identità virtuale, sarà compito del legislatore adottare le più opportune soluzioni affinché l'individuo possa esplicare la propria attività in un contesto comunque garantito e regolato. Sorge pur sempre la necessità di disciplinare i

¹² *Ibidem*, *passim*.

¹³ N. IRTI e E. SEVERINO, *Dialogo su diritto e tecnica*, Roma-Bari, 2001. Sui risvolti sociali del progresso tecnologico e sulle sue ricadute sul piano giuridico v. V. FROSINI, *Il diritto nella società tecnologica*, Milano 1981, p. 202. Sui rapporti tra informa-

tica e diritto si veda la recente pubblicazione di G. CORASANITI, *Il diritto nella società digitale*, Milano, 2018, dove il giurista, partendo da una ricostruzione sistematica sulle comuni radici della disciplina giuridica e informatica, evidenzia le similitudini e la costante e reciproca interazione.

comportamenti e le attività al fine di non rendere tutto ciò che è tecnologicamente possibile, solo per questo, giuridicamente legittimo¹⁴.

Purtuttavia, il giurista deve dunque porsi di fronte al nuovo che avanza in una diversa prospettiva, in cui le classiche categorie concettuali non sarebbero un *a priori* nel procedimento operativo dell'interprete, ma semmai uno strumento di passaggio per pervenire ad un risultato plausibile¹⁵. A un'innovazione tecnologica come quella in atto corrisponde un cambio di paradigma, non solo economico, ma anche sociale, e, impone, quindi, al giurista un mutamento di prospettiva rispetto ai classici criteri classificatori¹⁶ per dare risposta alle istanze sociali di tutela e certezza del diritto nelle relazioni.

La dottrina da tempo, con riferimento ai contratti informatici, nell'accezione ampia di contratti di utilizzazione degli strumenti dell'informatica e di contratti di acquisizione, elaborazione e diffusione di dati a mezzo di strumenti informatici¹⁷, si è interrogata sulla necessità di una creazione dogmatica di una nuova ed autonoma categoria contrattuale caratterizzata dall'avere ad oggetto beni o servizi dell'informatica¹⁸. Per alcuni, infatti, l'enu-

¹⁴ Efficacemente U. Galimberti rileva che “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 nutrive l'età umanistica e che ora, nell'età della tecnica, dovranno essere reconsiderati, dismessi o rifondati alle radici”. In U. GALIMBERTI, *Psiche e techne - L'uomo nell'età della tecnica*, Milano, 1999.

¹⁵ N. LIPARI, *Le categorie del diritto civile* (Milano 2013), 2013, p. 33.

¹⁶ Le categorie giuridiche orientando il processo interpretativo-applicativo, entro i limiti del caso, e in virtù di quest'ultimo, sono soggette a revisione, correzione ed integrazione. Sul punto G.B. FERRI, *Le stagioni del contratto e il pensiero giuridico di G. Alpa*, in *Riv. dir. comm.*, 2013, p. 215.

¹⁷ In dottrina, vi è chi, (SCUERSO, *Il contratto telematico. Le moderne tecnologie e il “vecchio” codice civile*, in www.aicisweb.it/documenti/2012/, p. 1) distingue tra contratti digitali, quali contratti stipulati con firma elettronica; telematici, ove conclusi mediante strumenti telematici tra assenti; ed informatici, se aventi ad oggetto beni e servizi di tipo informatico.

Altra dottrina si limitano a disquisire di contratti virtuali (E. Tosi, *Il contratto virtuale (parte 1)*, in *Studium Juris*, 2008, p. 670, distinguendo fra virtualità in senso proprio (contratto stipulato dall'utente per il tramite di un sito *web* predisposto da un professionista) e senso improprio (ricomprendente anche la contrattazione via mail). Secondo il citato Autore il contratto virtuale in senso improprio contemplerebbe i contratti conclusi via mail, rilevando Altri ancora sogliono distinguere tra contratti a conclusione informatica (L. FUERGUELE, *I contratti a conclusione telematica*, in F. BOCCHINI, *Diritto dei consumatori e nuove tecnologie*, I, *Gli scambi*, Torino, 2002, p. 145 ss.), ad oggetto informatico (In primis G. FINOCCHIARO, *I contratti ad oggetto informatico*, Padova, 1993; nonché R. PICARO, *I contratti ad oggetto informatico*, in F. BOCCHINI, *Diritto dei consumatori*, cit., p. 88 ss.) ad esecuzione informatica (R. PICARO, *I contratti ad esecuzione informatica*, in F. BOCCHINI, *Diritto dei consumatori*, cit., p. 207 ss.). Vi è infine chi propende per la categoria generale del contratto digitale (M. BIANCA, *I contratti*, cit., p. 1035 ss., e più di recente *Istituzioni di diritto privato*, Milano, 2014, p. 406, il quale, escluso che si tratti di un nuovo tipo, definisce telematico il contratto stipulato con strumenti informatici).

¹⁸ V. ZENO-ZENCOVICH, *Sul rilievo pratico o sistematico della categoria dei c.d.*

creazione di una categoria dei contratti di informatica sarebbe finalizzata ad identificare un nucleo minimo di elementi giuridici, comuni alla categoria individuata, in grado di trarre una maggior grado di certezza e regolazione dei rapporti ¹⁹. Sulla questione la prevalente dottrina è, tuttavia, orientata nel senso di escludere che una particolare conformazione tecnologica ed economica dell'oggetto della prestazione possa, di per sé sola, legittimare la cittadinanza di una categoria negoziale, posto che questo nuovo oggetto si innesta all'interno dei tradizionali schemi contrattuali senza perciò determinare un più generale quadro di riferimento normativo ²⁰. Se si è recentemente sopito il dibattito circa l'inquadramento giuridico del contratto informatico un nuovo terreno di confronto è sorto in riferimento ai contratti intelligenti, c.d. *smart contracts*, algoritmi scritti e programmati per eseguire (o essere essi stessi) un accordo intercorso tra le parti di un rapporto — in modo automatico e indipendentemente da un intervento umano — nel momento in cui vengono realizzate le condizioni predefinite nel protocollo medesimo. Appare evidente come la stessa definizione di *smart contract* evochi competenze e capacità afferenti al diritto e all'informatica. Il giurista ha, dunque, il compito di delineare il quadro normativo regolatorio di tutti quei comportamenti tecnologicamente possibili, che si dipanano attraverso l'utilizzo di tali nuove tecnologie. Dall'altro lato le nuove tecnologie contribuiscono al progresso giuridico, poiché impongono al legislatore di regolamentare nuovi comportamenti tecnologicamente possibili, laddove non si possa ricorrere ai classici schemi opportunamente adattati al nuovo contesto socio economico.

Lo spazio virtuale ²¹ (*cyberspace*), luogo in cui si collocano gli *smart contracts*, ha un proprio codice informatico, (linguaggio informatico) che lo definisce e lo regola, e dal quale discende una delle tante architetture possibili, allo stesso modo accade nello spazio reale, in cui il complesso delle norme giuridiche dettate dal legislatore definiscono, in un determinato territo-

contratti di informatica, in AA.VV., *I contratti di informatica. Profili civilistici, tributari e di bilancio*, a cura di Alpa G. e Zeno-Zencovich V., Milano, 1987, p. 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*, a cura di Alpa G. e Zeno-Zencovich V., Milano, 1987, pp. 373-375.

¹⁹ E. M. TRIPODI, *Formulario dei contratti d'informatica e del commercio elettronico*, 3° ed., Roma, 2002, p. 5.

²⁰ G. ALPA, *Sulla qualificazione dei "contratti di informatica"*, in *Econ. e dir. terziario*, Roma, 1989, 7.

²¹ Così definito poiché simula lo spazio "reale". Tuttavia, la realtà virtuale sta assorbendo quella reale, in un processo costante di assimilazione, dove è possibile esprimere la propria personalità al pari di quanto accada nel mondo reale. La rete si pone, quindi, come una realtà parallela alla vita reale o, per alcuni, risulterebbe essere un prolungamento della vita reale di un individuo.

rio, un dato ordinamento giuridico²². Il codice informatico o anche *lex informatica*²³ costituisce, quindi, un sistema di regole tecniche parallelo a quelle giuridiche, in cui il programmatore del codice detiene il potere regolatorio dello spazio virtuale²⁴, allo stesso modo del legislatore, con l'unica differenza dell'assenza, nello spazio virtuale, di limiti territoriali e di frontiere fisiche. Appare, pertanto, necessario conoscere le "regole tecniche" che governano la tecnologia esaminata, poiché, come vedremo, influenzano e limitano l'efficacia coattiva della norma a regolare le modalità di svolgimento delle relazioni che si svolgono in essa.

Diventa, quindi, essenziale conoscere le tecnologie per definire regolamentazioni attente alle potenzialità di intervento degli strumenti informatici²⁵. È, quindi, utile alla comprensione del nostro discorso illustrare, a grandi linee, le caratteristiche architetture della tecnologia blockchain, e delle sue componenti informatiche, nei limiti di quanto necessario per procedere alla disamina delle problematiche giuridiche già oggetto di vivaci dibattiti e tentare di tracciare, *de iure condito*, la cornice normativa entro la quale si collocherebbe tale nuova tecnologia.

2. I DISTRIBUTED LEDGER TECHNOLOGIES. DALLA BLOCKCHAIN PUBBLICA DEI BITCOIN ALLE BLOCKCHAIN PRIVATE: PROFILI TECNOLOGICI.

Sebbene il concetto di blockchain sia stato per la prima volta pienamente attualizzato nel *white paper* di Satoshi Nakamoto²⁶, nel quale viene sviluppata l'idea di una moneta digitale scambiata direttamente tra gli utenti²⁷, le sottostanti tecnologie dei suoi

²² "Il "codice" per l'informatico è "sorgente" (esattamente come per il diritto ci si riferisce comunemente alle "fonti" cioè ad una origine individuata di un flusso informativo costante) ed è nella sua essenzialità logica e condivisa il testo comprensibile di un algoritmo di un programma scritto in un linguaggio di programmazione da parte di un programmatore che si traduce in elaborato per arrivare a un programma "eseguibile" dal processore. Si tratta perciò di un punto di partenza ("sorgente") dell'intero processo che porta all'esecuzione del programma stesso (software) da parte dell'hardware della macchina, e che include altre fasi come la precompilazione, compilazione, interpretazione, caricamento e linking (a seconda del tipo di linguaggio di programmazione utilizzato)". In questo senso, G. CORASANITI, *Il diritto nella società digitale*, Milano, 2018, *passim*.

²³ Si v. J. REIDENBERG, *Reidenberg Lex Informatica: The Formulation of Informa-*

tion Policy Rules through Technology, in *Texas Law Review*, 1998, p. 553 ss.

²⁴ V. sul punto E. TOSI, *Contratti informatici, telematici e virtuali*, Milano, 2010, 14 e ss.

²⁵ In questo senso G. CORASANITI, *Il diritto nella società digitale*, cit., *passim*.

²⁶ Satoshi Nakamoto, *System for electronic transactions without relying on trust*, www.bitcoin.org. Nella versione italiana: "*Bitcoin: un sistema di moneta elettronica peer-to-peer*", www.bitcoin.org/bitcoin.pdf (siti consultati il 30 ottobre 2018).

²⁷ Per convenzione, il termine *Bitcoin*, con l'iniziale maiuscola, si riferisce alla tecnologia e alla rete, mentre il minuscolo *bitcoin* si riferisce alla valuta in sé. Cfr. M. BUSTILLOS, *The Bitcoin Boom*, The New Yorker, Condé Nast, 2013. L'aspetto importante del bitcoin, quale moneta digitale, non è solo il fatto che sia digitale, poiché, in circolazione, esistono altri tipi di monete digitali, sia esse regolamentate, come

componenti traggono ispirazione da anni di ricerca su crittografia, informatica ed economia.

Fino all'emersione di tale nuova tecnologia, si è ritenuto che solo le istituzioni, politiche ed economiche, come banche, società e governi, potessero porsi quali strumenti per ridurre l'incertezza e consentire gli scambi di valore o delle informazioni. La centralizzazione da parte di una singola autorità o entità comporta che dobbiamo fidarci di tali autorità, per mantenere l'ordine e la struttura all'interno della dimensione in cui operiamo. In concomitanza con l'esplosione della crisi finanziaria globale del 2007-2008 e l'emersione dei problemi legati alla centralizzazione del controllo è apparso il documento di Satoshi, il quale descrive un modo di scambiare una valuta, denominata bitcoin, che combina crittografia, informatica e teoria dei giochi nella sua progettazione e implementazione. La creazione di Satoshi permette a un partecipante di effettuare transazioni digitali direttamente con un altro partecipante (c.d. *peer to peer*) senza fare affidamento su un singolo intermediario centralizzato, come un istituto finanziario, al fine di convalidare i pagamenti.

Difatti, è noto che il classico trasferimento "elettronico" di denaro da un istituto finanziario ad un altro, a prescindere che avvenga recandosi allo sportello o tramite un app scaricabile sugli smartphone, comunque non interviene direttamente tra i conti di pagamento dei due soggetti interessati alla transazione, ma per il tramite dell'intermediazione di un terzo soggetto, quale appunto l'istituto finanziario autorizzato a tale scopo ²⁸.

Cosicché, l'aspetto dirompente del bitcoin, quale moneta digitale, non è stato solo il fatto di essere dematerializzata, poiché, in circolazione, esistono anche altri tipi di monete digitali, come la moneta elettronica ²⁹ emessa dalle banche e dagli istituti di mo-

la moneta elettronica, che non, ma risiede nella possibilità essere scambiato *peer to peer*, direttamente tra due soggetti, con un'infrastruttura minima e senza terze parti. Satoshi Nakamoto, spiega che: *"I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party"*.

²⁸ A differenza del pagamento in contanti, nei casi di trasferimento a mezzo strumenti elettronici, ci sarà una discrasia temporale, la cui ampiezza dipenderà dal tipo di mezzo di pagamento prescelto e dalla tecnologia utilizzata per il trasferimento dell'informazione di pagamento, che comporterà l'estinzione del debito in momento successivo a quello in cui il pagatore ha dato impulso al processo di pagamento. L'adempimento dell'obbligazione pecuniaria, *ex latere creditoris*, si avrà, quindi, con il tra-

sferimento "reale" della quantità di denaro, nel caso di moneta metallica e banconote, con la registrazione attiva sul conto del beneficiario o con il trasferimento telematico di bit da un wallet ad un altro, nel caso di trasferimento di disponibilità monetarie espresse in moneta elettronica. Per una ampia panoramica sulle modalità di estinzione dell'obbligazione pecuniaria si rinvia a M. GIULIANO, *"L'adempimento delle obbligazioni pecuniarie nell'era digitale. Dalla moneta legale alla moneta scritturale e digitale "legalmente" imposta"*, Torino, 2018.

²⁹ L'art. 1, co. 2, lett. h ter), TUB, così come novellato dal d.lgs. n. 45/2012, definisce la moneta elettronica come quel "valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso per ef-

neta elettronica ³⁰, ma la possibilità di trasferire unità di valore *peer to peer*, con un'infrastruttura minima e senza terze parti ³¹.

La tecnologia blockchain appartiene alla categoria delle tecnologie *Distributed Ledger* ³², caratterizzata da un registro impostato e strutturato in blocchi (contenenti più transazioni), che sono tra loro collegati in rete, in modo che ogni transazione eseguita nella rete debba essere validata sulla base di un processo basato sul consenso distribuito su tutti i nodi ³³.

La blockchain è, dunque, un *database* condiviso, decentralizzato, distribuito, immutabile (come precisato nel paragrafo 2.2), trasparente e criptato con precise regole di sicurezza, che registra l'insieme delle risorse e delle transazioni attraverso una rete *peer-to-peer*. Il *database* è aperto a tutti i partecipanti, salvo i casi di blockchain private, replicato su ogni computer che usa la rete, che può essere modificato solo attraverso l'esecuzione dello specifico algoritmo del consenso, previsto dal protocollo informatico.

La blockchain se da un lato è politicamente e architettonicamente decentralizzata, perché nessuno dei partecipanti ha un controllo singolare sulla stessa, e perché la sua infrastruttura non ha un punto centrale di fallimento, poiché ogni nodo conserva una copia della blockchain, dall'altro lato è anche logicamente centralizzata perché il sistema si comporta come un computer nonostante sia distribuito su tutti i nodi partecipanti nella rete.

La caratteristica della decentralizzazione consente alla blockchain di essere piuttosto resistente agli attacchi in quanto se uno o più nodi smettono di funzionare comunque può fare affidamento sugli altri nodi. Inoltre, a differenza dei sistemi centralizzati, dove la figura dell'amministratore funge da punto cardine di ogni istanza degli utenti e dove la conservazione è effettuata a

effettuare operazioni di pagamento come definite all'articolo 1, comma 1, lettera c), del decreto legislativo 27 gennaio 2010, n. 11, e che sia accettato da persone fisiche e giuridiche diverse dall'emittente".

³⁰ Si tratta di intermediari finanziari non bancari introdotti con la prima direttiva sulla moneta elettronica, la 2000/46/CE del 18-9-2000, la c.d. *electronic money directive*, e autorizzati ad emettere moneta elettronica.

³¹ "I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.": Satoshi Nakamoto.

³² Le *Distributed Ledger Technology* o DLT possono essere definite come un insieme di sistemi concettualmente caratterizzati dal fatto di fare riferimento a un registro distribuito, governato in modo da con-

sentire l'accesso e la possibilità di effettuare modifiche da parte di più nodi di una rete.

V. M. BELLINI, *Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia*, in <https://www.blockchain4innovation.it/esperiti/blockchain-perche-e-cosi-importante/>.

³³ Alla base del funzionamento di un registro distribuito decentralizzato c'è un meccanismo di consenso, ovvero un accordo tra diversi nodi che partecipano alla rete, al fine di validare le transazioni inserite nel *ledger*. Non esiste semplicemente un unico algoritmo di consenso, ma, generalmente, tre macrogruppi: *decentralized consensus*, *somewhat decentralized consensus* e *consortium consensus*. Si v. C. CACHIN, E. ANDROULAKI, A. D. CARO, M. OSBORNE, S. SCHUBERT, A. SORNIOTTI, M. VUKOLIC, AND T. WEIGOLD, *Blockchain, cryptography, and consensus*, <https://cachin.com/cc/talks/20161004-blockchain-techtuesday-web.pdf>, 2016, sito consultato il 30.10.2018.

livello unico, con conseguente rischio di un'eventuale perdita di dati, nei sistemi distribuiti ogni nodo è depositario di una copia del registro e ogni modifica è soggetta all'approvazione dell'intera comunità dei nodi, secondo le "regole" (informatiche) del consenso stabilite nell'algoritmo. Tuttavia, proprio per la caratteristica strutturale del sistema, nei database distribuiti i dati sono visibili ad ogni nodo, al contrario di quelli custoditi in quelli centralizzati che sono accessibili esclusivamente all'amministratore di sistema o a coloro che ne hanno i privilegi.

Nella blockchain e, in genere, nei DLT, la governance è costruita attorno ad un nuovo concetto di fiducia, dove il processo decisionale si realizza attraverso un meccanismo di costruzione del consenso distribuito tra tutti i soggetti partecipanti alla rete. Grazie a tali caratteristiche la blockchain è la tecnologia abilitante che consente di migliorare i modelli operativi dell'industria, ottimizzando le transazioni lungo la *supply chain*, nella gestione e verifica delle identità degli utenti, nell'amministrazione e nella gestione dei pagamenti tra le imprese e i consumatori, riducendo, al contempo i costi transattivi e il tempo di gestione dei processi aziendali.

Walmart ³⁴, il colosso americano della grande distribuzione al dettaglio, con oltre 11.000 negozi, ha avviato già a partire dal 2017, con la collaborazione di IBM, un progetto che vede l'utilizzo della blockchain per la tracciabilità dell'approvvigionamento alimentare e in genere dei prodotti alimentari. L'utilizzo di tale nuova tecnologia, si ritiene, aiuterà a individuare la fonte di contaminazione degli alimenti e contribuirà a migliorare la sicurezza pubblica riducendo i tempi per il riconoscimento delle patologie. Inoltre, la stessa azienda ha presentato un brevetto presso l'*U.S. Patent & Trademark Office* (USPTO) riguardante un sistema blockchain per le consegne, che consentirà di gestire il processo di registrazione dei segnali relative alle consegne dei pacchi provenienti da robot autonomi domestici o droni.

2.1. Segue. *La crittografia in uso nella Blockchain Bitcoin* ³⁵.

Uno degli aspetti più interessanti della blockchain è l'utilizzo della crittografia ³⁶ poiché garantisce, soddisfatte certe condizioni, che i messaggi trasmessi non vengano modificati e che si

³⁴ <https://www.technologyreview.com/the-download/612197/with-walmarts-veggie-tracker-blockchain-for-supply-chains-will-finally-get-real/>; <https://www.mark-up.it/walmart-blockchain-fornitori-verdura/>. Siti consultati il 30.12.2018.

³⁵ Per convenzione, il termine Bitcoin, con l'iniziale maiuscola, si riferisce

alla tecnologia e alla rete, mentre il minuscolo bitcoin si riferisce alla valuta in sé. Ci si riferisce, inoltre, alla Blockchain dei bitcoin con l'iniziale maiuscola. Cfr. M. BUSTILLOS, *The Bitcoin Boom*, cit.

³⁶ Il termine crittografia viene dalle parole greche *kryptos* che significa nascosto, e *graphia*, che significa scrittura.

possa stabilire, con assoluta certezza, il loro vero autore. Con la crittografia si possono proteggere le informazioni depositate sul proprio computer, proteggere le informazioni durante la trasmissione in rete e verificare l'integrità del documento ricevuto ³⁷. La crittografia è una tecnica in circolazione da molto tempo. Giulio Cesare la utilizzava per mantenere le comunicazioni militari private ³⁸.

Con il passare del tempo, gli algoritmi di cifratura, cioè le funzioni che eseguono le trasformazioni, sono diventati molto complessi e sicuri, sfruttando tecniche raffinatissime per sostituire, trasporre, aggiungere altre lettere, in modo da rendere incomprensibile il messaggio. La crittografia in uso nella blockchain utilizza un algoritmo per codificare i messaggi prima di inviarli, in modo che appaiono incomprensibili da coloro con i quali non si condivide l'algoritmo o non lo riesce a comprendere.

Nella rete Internet i messaggi viaggiano senza alcuna sicurezza crittografica. Chiunque lungo il percorso del traffico Internet può intercettare e leggere i messaggi che vengono scambiati. È come spedire una cartolina a mezzo del servizio postale, dove chiunque, se vuole, può leggere il contenuto. Esiste tuttavia un modo per scambiarsi messaggi su una rete pubblica non criptata con la sicurezza che nessuno possa leggerli al di fuori del destinatario. Tale risultato è possibile ottenerlo attraverso la crittografia a chiave pubblica o crittografia asimmetrica, nella quale si impiegano cifrari che fanno uso di due chiavi diverse, univocamente correlate: una serve per cifrare il testo chiaro, la chiave pubblica che il soggetto può condividere con chiunque desideri inviargli un messaggio, una per decifrare il testo cifrato con la prima, la chiave privata, che tiene per sé. Tale meccanismo tecnico di cifratura è alla base della firma digitale ³⁹, una procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la

³⁷ Quando condividiamo dati su Internet si corre sempre il rischio che possano essere copiati all'infinito. Se ciò non costituisce un problema per la condivisione di semplici informazioni, diventa problematico se ad essere copiata sia un'unità di valore rappresentativa di un certo potere d'acquisto, come nel caso del bitcoin o di un dato che consenta lo sfruttamento di uno specifico diritto o dà accesso ad un determinato contenuto.

³⁸ La tecnica utilizzata dall'imperatore romano consisteva nella sostituzione delle lettere, ad esempio sostituendo semplicemente ad una lettera quella che la segue di tre posizioni nell'alfabeto, come illustrato nel seguente esempio:

Originale: A B C D E F G H I L M N O P
Q R S T U V Z

Cifrato: E F G H I L M N O P Q R S T
U V Z A B C D

³⁹ Vedi *infra* per la definizione.

provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici ⁴⁰.

La chiave pubblica viene così chiamata perché può essere condivisa apertamente, ad esempio, perché inviata lungo la rete ad un altro soggetto. Essa, tuttavia, se può crittografare un messaggio non lo può decodificare. Solo la corrispondente chiave privata può decodificare o sbloccare i messaggi codificati con la chiave pubblica, motivo per quale deve restare segreta. Occorre inoltre segnalare che se da un lato la chiave privata viene ricavata dalla chiave pubblica utilizzando un complicato algoritmo matematico, è, invece, molto difficile invertire l'algoritmo per ottenere l'opposto.

L'utilizzo della crittografia asimmetrica permette, quindi, la segretezza delle informazioni scambiate e/o l'autenticazione del destinatario. Infatti, la segretezza e autenticazione del messaggio potrebbero essere perseguite laddove il medesimo messaggio venisse dapprima criptato con la chiave pubblica del destinatario e ulteriormente criptato con la chiave privata del mittente. Con questa tecnica il mittente avrà la certezza che il messaggio venga letto solo dal destinatario, poiché, questi, per poter leggere il messaggio, dovrà decriptarlo con entrambe le chiavi, quella sua privata e quella pubblica del mittente, e potrà avere la certezza che il messaggio non è stato alterato e che proviene esattamente dal soggetto possessore di quella determinata chiave privata. L'identità digitale e il processo di autenticazione fanno sì che possa dirsi che una persona che si presenti con una data identità sia effettivamente quella di chi o di cosa dice di essere.

Purtuttavia, nella blockchain, specie in quella pubblica, *nobody knows you're a dog* ⁴¹, poiché sebbene rispetto ad Internet si conosca la chiave pubblica di ciascun utente che partecipi ad una transazione, tuttavia tale informazione non consente la diretta riferibilità ad uno specifico soggetto, a meno che non si è grado di attivare un'attività investigativa capace di rintracciare la provenienza della chiave.

⁴⁰ Il principio della crittografia a chiave pubblica è stato ideato nel 1976 da Whitfield Diffie e Martin L. Hellmann. Successivamente, Ronald L. Rivest, Adi Shamir e Leonard M. Adleman hanno ideato nel 1977 il più noto ed oggi utilizzato sistema, denominato RSA, dalle iniziali dei loro cognomi. Per un'analisi approfondita si rinvia a PAAR C., PELZL, J. (2010). *Understanding Cryptography: A Textbook for Students and Practitioner*, Springer; Simmons, G.J. (a

cura di) (1992). *Contemporary Cryptology: The Science of Information Integrity*, IEEE Press-Wiley.

⁴¹ Il 5 luglio 1993, sulla rivista *The New Yorker*, apparve una vignetta di Peter Steiner che raffigurava due cani: uno seduto su una sedia di fronte a un computer, che si rivolgeva ad un secondo cane seduto sul pavimento, dicendo: "Su Internet, nessuno sa che sei un cane".

2.2. Segue. *La funzione hash nella tecnologia blockchain e il processo di validazione delle transazioni.*

Il sistema di cifratura asimmetrica richiede operazioni di calcolo molto elaborate e richiedono un tempo maggiore rispetto alla cifratura simmetrica. Cosicché per velocizzare ed efficientare il processo la chiave asimmetrica si suole applicarla non all'intero documento, ma solamente alla sua "impronta" o "digest" detta hash.

Una funzione di hash è un meccanismo digitale che viene utilizzato per comprimere i dati in un formato specifico di una lunghezza determinata. Nello specifico, l'impronta hash è una sequenza di lettere e cifre, ottenuta applicando un particolare algoritmo di calcolo alla sequenza di *bit* che formano il *file* o il testo⁴². Questo algoritmo non fa altro che scandire sequenzialmente uno dopo l'altro tutti i *byte* che costituiscono il file e ricavare, passo dopo passo, una serie di "impronte intermedie", ciascuna delle quali dipende dalla precedente, ottenendo, al termine della scansione, l'impronta hash definitiva. Ogni passo dell'elaborazione è influenzato da quelli precedenti e determina lo stato di quelli successivi, e per questo motivo è sufficiente modificare anche un solo *bit* di tutto il file per ottenere un'impronta hash diversa. Quindi, per verificare se un testo è stato modificato non occorre confrontare parola per parola i testi scambiati, ma basta solo verificare che gli hash dei due testi a confronto corrispondano. Un'altra caratteristica dell'impronta hash è quella di non permettere di risalire al testo originario. L'algoritmo di hash, infatti, è congeniato in modo da non consentire a nessuno di capire cosa abbia generato una determinata impronta. Non esiste infatti alcun algoritmo di decodifica che possa "svelare", ad esempio, che dietro alle impronte hash via sia una determinata parola.

Nella blockchain l'hash viene utilizzato per creare un collegamento tra ciascun blocco specifico. Questo si ottiene scrivendo l'hash di ogni blocco precedente nel blocco successivo della catena. Quando viene creato un blocco, viene creato un hash dei dati al suo interno e l'hash che viene creato include l'hash del blocco precedente. Se un pezzo di dati viene modificato in qualsiasi blocco precedente che fa parte della catena, ogni hash successivo cambierà. Il cambiamento passa a cascata, consentendo il rilevamento delle modifiche a qualsiasi parte di dati all'interno della catena confrontando gli hash dei blocchi tra loro

⁴² Tutti i tipi di dati, anche quelli più complessi, come ad esempio un video, una foto, che occupano una importante quantità di spazio, non sono altro che sequenze di 1 e 0, elaborati dalla funzione di hash in una stringa esadecimale a 256-bit, composta da numeri e lettere.

L'hash sha256('Bitcoin') è b4056df6691f8dc72e56302ddad345d65fead3ead9299609a826e2344eb63aa4.

L'hash sha256('bitcoin') è 6b88e087247aa2f07ee1c5956b8e1a9f4c7f892a70e324f1bb3d161e05ca107b.

attraverso i nodi della rete. Ciò impedirebbe le modifiche alla blockchain dopo che i blocchi siano stati creati e accettati dalla rete, salvo quanto si dirà appresso.

Quindi creato l'hash del documento, lo si può “firmare” usando la propria chiave privata e, quindi, inviare al destinatario, che, a sua volta, dal momento che la chiave privata è nota solo a colui che l'ha creata, il destinatario presume che l'hash provenga dal soggetto titolare della chiave privata. A questo punto, il destinatario può quindi elaborare autonomamente un hash del documento e confrontarlo con quello che ha ricevuto per verificare se vi è la perfetta corrispondenza e, quindi, che nessuno lo ha alterato.

Con questo sistema, nel Bitcoin ⁴³, si firmano le criptovalute che si trasferiscono ad altri utilizzando la propria chiave privata. È chiaro che se qualcuno dovesse ottenere la chiave privata di un altro soggetto, sarebbe in grado di inviare le criptovalute di tale soggetto a sé stesso, e a sottrarle al “wallet” ⁴⁴ di un altro utente. La blockchain è la tecnologia che supporta i bitcoin, ma è, tuttavia, posta alla base anche di altri sistemi dove la criptovaluta non è il bitcoin, ma altri asset digitali nativi. La blockchain propria del bitcoin è costituita da un insieme di transazioni raggruppate in blocchi, validati e aggiunti alla catena all'incirca ogni 10 minuti. I partecipanti alla rete sono *server* chiamati “nodi” che effettuano le transazioni aventi ad oggetto una certa quantità di criptovaluta. Quando i bitcoin vengono scambiati passano da un indirizzo informatico ad un altro ⁴⁵. Il procedimento di generazione di un blocco, nel quale vi sono i dati relativi alle transazioni confermate di bitcoin in un dato intervallo di tempo, inizia con la creazione di una transazione da parte di un nodo, per la quale viene dapprima calcolato il *digest* applicando la funzione di hash (nel cui calcolo è incluso anche il *timestamp* della transazione), al fine di garantirne l'integrità e autenticità, e poi firmata digitalmente con la propria chiave privata, al fine di dimostrarne la titolarità a spenderne una certa quantità ⁴⁶. Quindi, nell'ipotesi di un trasferimento di bitcoin tra Alice e Bob, Alice

⁴³ L'algoritmo di hashing utilizzato dalla blockchain di Bitcoin è SHA-256, che sta per *Standard Hashing Algorithm*, con una lunghezza hash di 256 bit. In questo hash, i dati hash sono sempre lunghi 256 bit.

⁴⁴ Il c.d. *wallet* in genere è un software che consente di gestire il proprio “salvadanaio” di criptovalute. Un *wallet* normalmente gestisce uno o più indirizzi bitcoin o altra valuta e per ognuno di questi conserva la chiave privata senza la quale non sarebbe possibile spendere i relativi bitcoin. Ci sono vari tipi di *wallet*, alcuni gestiscono

le operazioni nel computer dell'utente mentre altri sono solo delle interfacce a dei servizi remoti.

⁴⁵ L'indirizzo bitcoin può essere paragonato al codice IBAN di un conto corrente bancario; si tratta di un numero intero che si ricava partendo dalla chiave pubblica.

⁴⁶ Allo scopo di agevolare il calcolo dell'hash, il sistema include nell'intestazione un campo unico che contiene un singolo hash ottenuto dai dati di tutte le transazioni (txid) incluse in quel blocco. I txid sono accoppiati due a due, creando un hash

aggiunge la chiave pubblica di Bob, affinché questi possa successivamente spendere la disponibilità di asset ricevuti, e trasmette la transazione agli altri nodi della rete affinché la possano verificare. La transazione viene quindi validata da un nodo c.d. *miner*⁴⁷ e inclusa in un blocco di transazioni registrato sulla blockchain. A questo punto la transazione, una volta confermata da un numero sufficiente di blocchi consecutivi, verrà permanentemente agganciata alla blockchain e accettata come valida da tutti i partecipanti. È opportuno evidenziare che le transazioni sono rappresentate da una struttura di dati che codifica e trasferisce un valore che non è relazionato a nessun conto ma è legato esclusivamente all'identità di un soggetto rappresentata dalla sua chiave pubblica. Per validare i blocchi è necessaria una prova di lavoro, c.d. *proof of work* che i nodi *miner* devono presentare al fine di ottenere la ricompensa. Si tratta di risolvere un problema crittografico molto complicato, che richiede una quantità di calcolo molto elevata e, dunque, una spesa in energia elettrica. Grazie a questo meccanismo si evita di incorrere nel rischio del *double spending*. Difatti, Alice può inviare un messaggio a Bob attraverso il semplice uso di firme digitali, senza dover passare per la blockchain. Tuttavia, Alice potrebbe spedire lo stesso messaggio a più soggetti, spendendo più volte quell'informazione (ad es. unità di valore). Per evitare tale inconveniente, in assenza di un'autorità centrale che tenga traccia del trasferimento, interviene la blockchain il cui protocollo prevede che tutti tengano una copia di tutte le transazioni e che possano verificare che il secondo pagamento è illegittimo.

Il problema crittografico da risolvere consiste nel trovare un *nonce*, ovvero un hash per il blocco, che inizi con un certo numero di zeri. Attualmente sulla blockchain di Bitcoin, i minatori devono trovare hash a partire da 19 zeri. È difficile come rotolare i dadi a 36 facce e ottenere tutti i sei⁴⁸.

per ogni coppia di transazioni. Ogni hash viene poi accoppiato con un altro hash, creando un hash figlio dei due hash precedenti, e così via finché non si arriva a un unico hash. Tutti gli hash sono riorganizzati in una struttura dati ad albero detta *Merkle Tree*, dove le foglie sono le transazioni txid, i rami (sono due ogni passo) gli hash intermedi e la radice l'hash finale, *Merkle root*, prodotto di tutti gli altri hash. Il vantaggio principale degli alberi di *Merkle* è che quando il dato di un blocco cambia, non è necessario calcolare l'hash sopra ogni altro dato, ma si calcolano solamente i nodi lungo il ramo, fino al nodo radice. Così facendo il numero di calcoli hash richiesto diminuisce logaritmicamente sul numero di blocchi di

dati totali. Tale processo risulta essere particolarmente efficiente quando vi sono molte ramificazioni dell'albero. Tale concetto stato brevettato nel 1987 da Ralph Merkle e descritto nel paper "*A Digital Signature Based on a Conventional Encryption Function*". V. <https://people.eecs.berkeley.edu/~raluca/cs261-f15/readings/merkle.pdf>.

⁴⁷ I *miners* sono dei soggetti economici previsti ed economicamente incentivati dal sistema Bitcoin per controllare la "leicità" dei pagamenti disposti ed inviati nella rete dagli utenti, inserire gli ordini "leciti" nell'ultimo blocco, ovvero nell'intervallo temporale ancora "aperto", e sigillare tale blocco con un hash.

⁴⁸ Il protocollo Bitcoin adegua perio-

La caratteristica fondamentale del protocollo, che conferisce alle transazioni effettuate il carattere dell'immutabilità, è quella di includere l'hash del blocco precedente. In questo modo, i blocchi sono collegati fino al primissimo blocco di genesi e sono verificabili anche esse da un hash. In tal modo, poiché ogni blocco contiene l'hash precedente e quello che sarà contenuto nel blocco successivo, si giunge ad avere una catena per cui tutti gli hash precedenti vengono elaborati in tutti gli hash dei blocchi futuri. È qui che, dunque, entra in gioco la vera immutabilità. Tutti i blocchi sono collegati attraverso le interrelazioni di tutti i loro hash. Il meccanismo del consenso, di validazione delle transazioni, la già detta *proof of work*, rappresenta tuttavia il vero elemento che cambia il modo di processare i trasferimenti di valore nel sistema economico, poiché le parti fanno a meno di affidarsi ad un terzo soggetto garante dell'operazione. La sicurezza del sistema è data dal fatto che non è possibile sapere a priori quale sarà il nodo che risolverà il problema matematico, né quali saranno i nodi che poi verificheranno il risultato. Per alterare la catena dei blocchi è, quindi, necessario avere il controllo del 51% dei computer e ciò viene considerato (praticamente) impossibile.

Si comprende, dunque, quali siano le caratteristiche che rendono la blockchain così interessante nelle relazioni economiche: a) l'indelebilità delle transazioni una volta registrate in essa, b) l'invulnerabilità, integrità e sicurezza del registro, progettato per garantire in modo autonomo la "bontà" delle transazioni e c) l'affrancamento da una autorità centrale deputata alla gestione del registro o al controllo dell'accesso al registro stesso.

Tuttavia, tali caratteristiche non sono presenti, con la stessa rilevanza, in tutti i tipi di protocolli. Vediamo alcuni modelli.

2.3. Segue. *Le blockchain permissionless, permissioned e del tipo consortium* ⁴⁹.

Esistono diversi tipi di blockchain che implementano diversi livelli di autorizzazione per diverse categorie di partecipanti. La maggior parte di esse sono per lo più pubbliche, c.d. *permissionless ledgers*, come ad esempio Bitcoin ed Ethereum.

Il sistema Bitcoin (BTC) è stato progettato per inviare danaro in tutta sicurezza su Internet, senza necessità di intermediazione del

dicamente la difficoltà (e cioè varia il numero di zeri necessari) in modo tale che i *miner* impieghino mediamente sempre 10 minuti per risolvere il problema e sigillare il blocco. Se i *miner* investono in nuovi processori aumentano la loro potenza di calcolo allora i tempi medi di risoluzione del pro-

blema si riducono e quindi il protocollo aumenterà la difficoltà.

⁴⁹ C. CACHIN, E. ANDROULAKI, A. D. CARO, M. OSBORNE, S. SCHUBERT, A. SORNIOTTI, M. VUKOLIC, and T. WEIGOLD, *Blockchain, cryptography, and consensus*, cit.

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 ⁵⁰ (ETH) è una piattaforma decentralizzata che può essere scaricata gratuitamente e ha la capacità di essere programmata, simile a un computer. Un giovane programmatore russo-canadese, Vitalik Buterin, nel 2013, rendendosi conto delle potenzialità dei DTL e, in particolare della blockchain, ha deciso di sviluppare Ethereum, attraverso la quale i programmatori possono sviluppare applicazioni decentralizzate (*decentralized application*, dette “DApp” o “dApps”) senza dover “costruire” una nuova blockchain. Si tratta, nello specifico, di applicazioni eseguite su una rete blockchain ⁵¹, in questo caso quella di Ethereum, anziché su un computer centrale (modello server-client) come potrebbe essere il caso di Facebook, Apple e Twitter; sono completamente *open source*, utilizzano dati e *token* cifrati e non hanno alcuna entità che controlli la rete.

La caratteristica principale del protocollo Ethereum, che lo differenzia dal Bitcoin, risiede nella gestione dei contratti intelligenti, codici informatici che funzionano esattamente come programmato senza alcuna possibilità di inattività, censura, frode o interferenza da parte di terzi. Queste applicazioni, una volta lanciati nella blockchain, non possono essere modificati. Il vero elemento innovativo di tale protocollo è dato dall’Ethereum Virtual Machine o EVM: si tratta di un ambiente di *runtime* per lo sviluppo e la gestione di *smart contracts*, completamente separato dalla rete, in modo da operare in un ecosistema tutelato da interferenze esterne. Con la blockchain di Ethereum è possibile creare una rappresentazione digitale di qualsiasi bene o idea, sottoforma di *token* ⁵².

⁵⁰ Tom Lyons, direttore di Consensus, una organizzazione globale che si propone di costruire e diffondere infrastrutture, applicazioni e pratiche che abilitano un mondo decentralizzato, in un’intervista rilasciata al *lsole24ore* il 12.11.2018, spiega che se con blockchain intendiamo una piattaforma per “database distribuiti”, Ethereum è una piattaforma per “computing distribuito”. Il progetto nasce e si sviluppa come una blockchain pubblica nella forma di piattaforma di *distributed computing open source*. Non è solo una moneta digitale, ma è stata concepita per sviluppare progetti tecnologici, per favorire lo sviluppo di nuove criptovalute, che per l’appunto si appoggiano nella fase di startup (Ico) sulla rete

Ethereum (V. <https://www.ilsole24ore.com/art/tecnologie/2018-11-12/blockchain-sopravalutata-storytellers-e-detraitori-tecnologia-piu-discussa-sempre-143604.shtml?uuid=AEv8aVdG>, 12.11.2018).

⁵¹ Tali applicazioni, tuttavia, non devono necessariamente essere eseguite su una blockchain. Ci sono, infatti, applicazioni come BitTorrent e Tor che funzionano su una classica rete *peer to peer*.

⁵² I *token* sono una rappresentazione informatica di una particolare risorsa o utilità, che di solito risiede sopra un’altra blockchain. La creazione di *token* è un processo piuttosto semplice, in quanto non è necessario modificare i codici di un particolare protocollo o creare una nuova

L'idea di utilizzare la blockchain in specifiche filiere, nel sistema finanziario, nei pagamenti, ha portato alla nascita di infrastrutture chiuse, in grado di essere conformi al contesto normativo in cui devono operare ⁵³.

Sono state quindi sviluppate altre tipologie di blockchain come quelle del tipo “*consortium*” o a “permesso condiviso”, o dette anche “parzialmente decentralizzata”, in cui il processo di consenso è controllato da un insieme preselezionato di nodi, e quelle “private”, c.d. *permissioned ledgers*, accomunate, entrambe, dalla presenza di nodi preselezionati che svolgono la funzione di validatori, ancorché vi possa essere l'ipotesi in cui sia consentito l'accesso a tutti i nodi per la mera visualizzazione del registro (*permissioned* pubblico). Cosicché, mentre nelle blockchain pubbliche a chiunque è consentito scaricare il software e creare un nodo, solo in quelle *permissionless* tutti i nodi possono partecipare al processo di validazione delle transazioni, mentre nelle blockchain appartenenti a un consorzio o private la partecipazione è solitamente consentita solo ai nodi specificamente autorizzati (*permissioned* privata).

Cosicché, nel consorzio potremmo avere, ad esempio, un gruppo di soggetti, che gestiscono i nodi, in modo che tutte le entità sono abilitate a firmare le transazioni e sono in grado di accedere e controllare il registro senza bisogno di accedere ai registri interni degli altri membri. Questo potrebbe essere considerato un ambiente a bassa fiducia. Le organizzazioni si fidano l'una dell'altra, ma non hanno una completa fiducia. Questa tipologia di blockchain può essere anche pubblica, cioè scaricabile su qualsiasi computer in modo che chiunque possa vedere le informazioni processate dai blocchi, senza che, tuttavia, tutti i partecipanti abbiano i privilegi per partecipare attivamente al consenso, poiché il processo di consenso è controllato da un numero predefinito di nodi. Esempi di tale tipo blockchain è Il consorzio R3 CEV LLC, una società finanziaria e di ricerca tecnologica. Coopera con un consorzio di

blockchain. L'interesse per il bitcoin probabilmente si è particolarmente intensificato con l'ascesa del fenomeno delle ICO (*Initial Coin Offer*), gestite attraverso offerte di *token*, correlati ad un determinato progetto o iniziativa imprenditoriale. Circa il funzionamento delle ICO si veda il rapporto pubblicato dalla società di ricerca *Autonomous Research*, in <https://next.autonomous.com/download-token-mania>, nel quale per spiegare il meccanismo utilizza l'esempio del progetto di apertura di un nuovo Casinò e la decisione dei proprietari di finanziarne la costruzione attraverso la vendita anticipata delle *fiches* ed il riconoscimento ai finanziatori del diritto di utiliz-

zarle al di fuori per creare valore attraverso l'avvio degli scambi. I finanziatori acquistano le *fiches*, da un lato, finanziano in modo diretto la costruzione del Casinò apportando liquidità e dall'altro, cominciando ad operare scambi con le *fiches*, contribuiscono (insieme alla validità e solidità del progetto stesso) a far raggiungere indirettamente a queste il valore atteso e prefissato nel progetto.

⁵³ Si pensi all'obbligo della rintracciabilità di tutti gli alimenti e mangimi, introdotto dal Regolamento (CE) 28 gennaio 2002, n. 178 del Parlamento europeo e del Consiglio, o alle prescrizioni imposte dalla legislazione antiriciclaggio o quelle dettate a tutela della protezione dei dati personali.

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. Il consorzio ha creato una *open source distributed ledger platform* chiamata Corda ⁵⁴, particolarmente rivolta al mondo finanziario in quanto gestisce transazioni più complesse e limita l'accesso ai dati delle transazioni. Altro progetto del tipo consorzio è *Hyperledger*, un progetto della Fondazione Linux ⁵⁵ 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. Tra i progetti di Hyperledger vi è *hyperledger Fabric* ⁵⁶, che è tuttavia una tipo di blockchain privata, originariamente fornita da IBM e *Digital Asset*, che fornisce un'architettura modulare con una delineazione dei ruoli tra i nodi dell'infrastruttura, in grado di consentire l'esecuzione degli *smart contracts* (denominati "*chain-code*"), la configurazione del consenso e i servizi di appartenenza.

Le blockchain private, invece, fanno un ulteriore passo in avanti. In una blockchain privata c'è generalmente un alto grado di fiducia. Questo è molto più simile a un sistema centralizzato, ma fornisce un alto grado di verificabilità dal momento che le transazioni sono visualizzabili solo per coloro che hanno avuto accesso. Ogni DTL implementa regole proprie che vengono scritte in conformità con gli obiettivi perseguiti. In quelle private non si ricorre alla *proof of work* pur mantenendo, in ogni caso, i requisiti di protezione e certezza dei dati registrati ⁵⁷. Appare evidente, quindi, che in tali ambienti, potendo fare affidamento sull'identità dei partecipanti, si possono utilizzare meccanismi di

⁵⁴ <https://www.corda.net/index.html>.

⁵⁵ <https://www.linuxfoundation.org>.

⁵⁶ <https://www.hyperledger.org/projects/fabric>. Il progetto *Hyperledger* è costituito da dieci differenti piattaforme, una delle quali è *Fabric*, una *permissioned private* blockchain promossa da IBM. La caratteristica principale della blockchain di *Hyperledger Fabric* è il fatto di essere privata e ad accesso controllato. Per garantire queste proprietà è necessario che gli attori che partecipano alla rete siano dotati di identità digitale.

⁵⁷ Esempi di blockchain private è Chain (<https://chain.com>) si tratta di una società tecnologia che collabora con diverse organizzazioni per la creazione, l'installazione e l'utilizzo di blockchain private nell'ambito dei prodotti e dei servizi finanziari; Multichain (<https://www.multichain.com>) è

una piattaforma aperta per la creazione di blockchain private. Si noti che le prestazioni delle blockchain private e delle blockchain consorzio sono spesso migliori di quelle pubbliche, poiché non si basano su prove di lavoro per stabilire un consenso. Nell'ambito dei sistemi di pagamento vi è Ripple ("*Ripple Transaction Protocol*", in sigla RTXP o anche "Protocollo di transazione Ripple") un sistema di trasferimento di fondi in tempo reale, fornito dall'omonima società Ripple. Il protocollo è realizzato attorno ad una base di dati pubblica e condivisa, che usa un ambiente consensuale per pagamenti in un processo distribuito. La rete è decentralizzata, tra i "validators" ci sono società, *internet service providers* e il *Massachusetts Institute of Technology*. V. <https://gigaom.com/2014/09/24/two-us-banks-are-ready-to-embrace-the>

consenso meno onerosi della *proof of work*, ciò tuttavia a discapito dell'affidabilità del processo di validazione, proprio dei Bitcoin.

In estrema sintesi, la blockchain è una base dati distribuita tra tutti partecipanti alla rete, dove ogni voce contenuta nella base dati è matematicamente collegata alla voce precedente. La vera peculiarità della blockchain, tuttavia, consiste nel meccanismo di consenso, distribuito tra i nodi della rete, con il quale ciascuna transazione da un nodo ad un altro è convalidata. Con tale meccanismo di validazione, la catena di informazioni registrate nel registro distribuito diventa matematicamente sicura, a prova di manomissione, e rimuove i conflitti tra i diversi nodi partecipanti alla rete, tale per cui, all'interno del *network* non vi è possibilità di censura, prevaricazione di un partecipante sull'altro o di esclusione. Ciascun nodo è trattato allo stesso modo; il governo della rete non è più, quindi, gestito da un'autorità centrale, tipica di un sistema centralizzato, anche se distribuito, ma è sostituito da una rete decisionale globale, formata da nodi aventi gli stessi privilegi. Oltre alla *proof of work*, ci sono anche altri meccanismi di consenso, introdotti dagli sviluppatori per ovviare alla enorme potenza computazionale necessaria per risolvere il *puzzle* matematico proprio della "prova di lavoro" e per ridurre il tempo di attesa della validazione della transazione. Tra i vari sistemi ricordiamo la: *Proof of stake* (POS) ⁵⁸; *Delegate Proof of Stake* DPOS ⁵⁹; *Proof of Capacity* (POC) ⁶⁰; *Proof of Elapsed Time* (POET) ⁶¹. Per il resto, tutte le blockchain sono caratterizzate da una catena di blocchi, matematicamente collegati tra loro e validati in base a uno specifico meccanismo di consenso. Ed è questo meccanismo, oltre chiaramente al diverso grado di accessibilità alla rete, che porta, fondamentalmente, a distinguere la Blockchain dalle altre blockchain pubbliche, private o ibride.

Peraltro nella blockchain pubblica oltre all'assenza di permessi a partecipare al *network*, lo stesso codice sorgente è reso pubblico, proprio per consentire agli sviluppatori di tutto il mondo, previo raggiungimento del consenso, di modificarlo e migliorarlo ⁶². Al contrario, nelle blockchain private o consortili, solo i soggetti autorizzati possono partecipare alla rete e solo specifici

ripple-protocol-allowing-instant-global-money-transfers/ Two US banks are ready to embrace the Ripple protocol, allowing instant global money transfers, GigaOM, consultato in data 30.10.2018; *Tech Showcase: Ripple Labs*, Institute of International Finance, consultato in data 30.10.2018, <https://www.youtube.com/watch?v=DvBns7XLLxo>, consultato in data 30.10.2018.

⁵⁸ <https://en.wikipedia.org/wiki/Proof-of-stake>.

⁵⁹ https://it.wikipedia.org/wiki/Delegated_Proof_of_Stake.

⁶⁰ <https://en.wikipedia.org/wiki/Proof-of-space>.

⁶¹ <https://blockonomi.com/proof-of-elapsed-time-consensus/>.

⁶² Anche per aggiornare e modificare il codice sorgente è necessario raggiungere

nodi sono abilitati a partecipare al processo di consenso per validare le transazioni. Certamente, in tali tipologie di *distributed ledger* il controllo è disperso tra più nodi, ma in modo più limitato rispetto a quanto accade, in genere, nella blockchain pubblica, con l'ovvia ricaduta in termini di sicurezza dell'intero sistema. In tali casi probabilmente è improprio parlare di blockchain, poiché ci si allontana talmente tanto dal modello Bitcoin da assumere la configurazione di un *database* decentralizzato e parzialmente distribuito, con una o più autorità centrali che governano la rete. È come se riferendoci a Internet, parlassimo di "intranet", la rete interna aziendale che utilizza i *browser*, i *server* e i protocolli di comunicazione di Internet, a cui però possono avere accesso solo utenti autorizzati. Le alternative "regolate" alla Blockchain dovranno essere, dunque, in grado di replicare quanto questa è in grado di esprimere, ovvero una sicura alternativa alla fiducia riposta in un terzo, attraverso sistemi matematici e teoria dei giochi, grazie alle quali il partecipante che tenta di ingannare la rete dovrà impiegare un lavoro complesso, ma facile da controllare, tale che scongiuri ogni minaccia di alterazione dei dati, per cui è meglio giocare con le regole che contro le regole⁶³.

3. LE QUESTIONI GIURIDICHE: LA TECNOLOGIA BLOCKCHAIN E LA PROTEZIONE DEI DATI PERSONALI ALLA LUCE DEL REGOLAMENTO EUROPEO 2016/679.

Si è detto che la blockchain è sostanzialmente un *date base* distribuito su un gran numero di computer, c.d. nodi, nei quali vengono memorizzati i dati immessi da ciascun partecipante, al fine di dare seguito alle operazioni per le quali si è dato impulso. Appare evidente che l'architettura e le caratteristiche specifiche di ciascuna blockchain impattano sulle modalità di trattamento dei dati personali⁶⁴ e, quindi, sul diritto delle persone alla protezione degli stessi⁶⁵.

un consenso. Se non si raggiunge il consenso tra gli sviluppatori, il codice sorgente resta così com'è o si realizza una c.d. *Hard Fork*, ovvero una scissione che genera due blockchain distinte, ciascuna, quindi, con una propria e differente criptovaluta. Bitcoin Cash e Bitcoin Gold sono due nuove criptovalute, nate nel corso del 2017, per effetto della biforcazione della blockchain dei bitcoin.

⁶³ A. Antonopoulos, *Mastering Bitcoin*, USA, 2017, *passim*.

⁶⁴ L'art. 4 del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (*General Data Pro-*

tection Regulation o GDPR) definisce "dato personale" qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

⁶⁵ Il Parlamento Europeo, nella Risoluzione del 3 ottobre 2018 sulle "tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione (2017/2772(RSP))" sottolinea che è della

I caratteri principali che troviamo nella blockchain pubblica, ancorché con diverse declinazioni a seconda del tipo di blockchain utilizzata, sono la trasparenza, poiché tutti i partecipanti possono visualizzare tutti i dati inseriti anche dagli altri partecipanti; la condivisione e decentralizzazione, in quanto diverse copie della blockchain esistono simultaneamente su diversi computer; l'irreversibilità, in quanto una volta inserito un dato, non può essere modificato o cancellato; la disintermediazione, poiché ogni decisione è presa in ragione del consenso reso dai partecipanti, senza l'intermediazione di un'autorità centrale.

Tali caratteristiche dovranno evidentemente conciliarsi con i principi fissati nel GDPR, direttamente applicabile in tutti gli Stati membri, e con le norme contenute nel codice della privacy, recentemente adeguato al citato Regolamento, con il d.lgs. 10 agosto 2018, n. 101⁶⁶. Infatti, in tali disposizioni si afferma che il trattamento dei dati personali deve essere lecito, equo e trasparente; deve essere limitato allo scopo specifico per il quale sono stati originariamente raccolti; è possibile raccogliere solo i dati assolutamente necessari allo scopo specifico (c.d. minimizzazione dei dati); i dati devono essere accurati e aggiornati, non devono essere conservati più a lungo del necessario e devono essere elaborati in modo sicuro (integrità e riservatezza)⁶⁷. Partendo dalla definizione di “dato personale” contenuta nel Regolamento, non sembra che vi possano essere dubbi circa la natura di “dato personale” delle informazioni immesse nella blockchain, ancorché cifrate tramite la funzione hash e il sistema della crittografia asimmetrica. Tali sistemi, infatti, sono una tecnica di pseudonimizzazione che consente di trattare le informazioni di un soggetto in modo tale da impedirne l'identificazione. I dati immessi nella blockchain sono, dunque, dati pseudonimizzati, considerati dal regolamento come informazioni su una persona fisica identifica-

massima importanza che gli usi del DLT siano conformi alla legislazione dell'UE sulla protezione dei dati, in particolare al regolamento generale sulla protezione dei dati (GDPR) ed invita la Commissione e il Garante europeo della protezione dei dati (GEPD) a fornire ulteriori orientamenti su questo punto. Il Parlamento inoltre evidenzia che la DLT promuove la pseudonimizzazione degli utenti, ma non la loro anonimizzazione. Cosicché, se la pseudonimizzazione impedisce l'identificazione del soggetto senza l'utilizzo di informazioni aggiuntive, tuttavia non è una tecnica che impedisce in assoluto l'impossibilità di identificare la persona che si celi dietro il dato.

⁶⁶ Si veda CNIL, September 2018 “*Blockchain et RGPD: quelles solutions pour un usage responsable en présence*

de données personnelles?”, disponibile qui: <https://www.cnil.fr/fr/blockchain-et-rgpd-queles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles>, visitato il 30 ottobre 2018. Sull'analisi di conformità della blockchain in relazione al GDPR si veda anche Luis-Daniel IBÁÑEZ, Kieron O'HARA, and Elena SIMPERL, *On Blockchains and the General Data Protection Regulation*, reperibile all'indirizzo https://eprints.soton.ac.uk/422879/1/BLOCKCHAINS_GDPR_4.pdf, visitato il 30 ottobre 2018; Massimiliano NICOTRA, *Blockchain e GDPR: le norme da conoscere per tutti i problemi*, 24 luglio 2018 su <https://www.agendadigitale.eu/sicurezza/blockchain-e-gdpr-le-norme-da-conoscere-per-tutti-i-problemi/>, visitato il 30 ottobre 2018.

⁶⁷ Art. 5 GDPR.

bile, poiché ancorché non direttamente riconducibili a una persona fisica, lo possono essere con l'utilizzo di ulteriori informazioni ⁶⁸. Diverso è, invece il discorso per i dati anonimi, vale a dire "informazioni che non si riferiscono a una persona fisica identificata o identificabile" per i quali il regolamento trova piena applicazione.

Volgendo lo sguardo alla blockchain, i dati degli utenti, ancorché cifrati, non possono essere considerati anonimi, in quanto sebbene incomprensibili e destrutturati, potrebbero portare all'identificazione di un soggetto se abbinati ad altre informazioni. Sul punto è intervenuto il Gruppo di Lavoro ex art. 29, nel Parere 05/2014 ⁶⁹, il quale, con riferimento alla funzione hash ⁷⁰, rileva che se l'intervallo di valori di immissione relativi alla funzione di hash è noto, la funzione stessa consente di riprodurli al fine di desumere il valore corretto associato a un dato specifico ⁷¹. Se si utilizza, invece, la crittografia con chiave asimmetrica, la decrittazione comunque può avvenire, anche se si è venuti a conoscenza della chiave privata. Peraltro, finanche gli indirizzi IP dinamici ⁷², in una recente sentenza della Corte di Giustizia dell'Unione Europea ⁷³, sono considerati dati personali in circostanze in cui è possibile ottenere informazioni da una terza parte, in modo tale da consentire di identificare l'utente. Nella specie, secondo la CGUE, anche se un indirizzo IP dinamico non è di per sé sufficiente per identificare l'interessato, tale insieme di informazioni deve essere trattato come dato personale, qualora il soggetto che conserva l'indirizzo IP disponga dei mezzi giuridici che gli consentano di far identificare la persona interessata attraverso il ricorso alle informazioni detenute dal fornitore di accesso a Internet.

È pur vero che alcuni dei principi stabiliti dal Regolamento trovano sicura tutela nella blockchain, se si considera che tale tecnologia, è decentralizzata e distribuita e questo rende molto più difficile un attacco di *cybercrime*; le informazioni sulle transazioni, quali l'identità dei soggetti e gli altri dati personali, sono, come detto, pseudonimizzate, ancorché pubbliche e, quindi, noti

⁶⁸ Considerando n. 26.

⁶⁹ https://www.garanteprivacy.it/documents/10160/2133805/WP216+Opinion+05+2014+on+_Anonymisation+Techniques+onto+the+web.pdf, visitato il 30 ottobre 2018.

⁷⁰ Si ricorda che gli algoritmi usati nella funzione hash sono unidirezionali, poiché, di fatto, non consentono l'inversione al dato di partenza.

⁷¹ Effettuando l'hashing di tutti i possibili valori di immissione e raffrontando il risultato con i valori contenuti nell'insieme di dati.

⁷² Gli indirizzi IP "dinamici" sono quelli provvisori, ossia assegnati ad ogni connessione a Internet e sostituiti in caso di successive connessioni, a differenza degli indirizzi IP « statici », che sono invariabili e consentono l'identificazione permanente del dispositivo connesso alla rete.

⁷³ Breyer(C-582/14), si veda in: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=43862>, sito visitato il 30 ottobre 2018.

agli altri nodi; la crittografia utilizzata, in linea di principio, garantisce un metodo piuttosto sicuro per archiviare e gestire le informazioni.

Vi sono, tuttavia, altri principi fissati nella normativa europea che difficilmente potranno essere rispettati, come quello che sancisce il diritto alla cancellazione dei dati personali (c.d. diritto all'oblio) o anche alla loro rettifica, stante il carattere immodificabile della blockchain. A parte l'utilizzo di tecniche per anonimizzare i dati trattati nella blockchain, come nel caso di utilizzo di una coppia di chiavi per ciascuna transazione da parte del medesimo soggetto ⁷⁴, ad oggi la tecnologia in esame non consente l'esercizio di un tale diritto ⁷⁵.

Altra questione che si è posta concerne l'individuazione dei soggetti nei confronti dei quali gli utenti potrebbero chiedere il rispetto dei principi posti a tutela dei loro dati. È noto infatti che il GDPR e il codice della privacy individuano nel titolare (*data controller*) e responsabile del trattamento (*data processor*) i soggetti deputati a garantire i su richiamati principi. Lo stesso regolamento, peraltro, è stato pensato partendo dall'assunto che i dati siano controllati da soggetti identificati e identificabili. Si pone, dunque, un problema di *governance* del sistema tecnologico, tenuto conto che la conformità al GDPR non riguarda la tecnologia, ma piuttosto come la tecnologia viene utilizzata per elaborare i dati personali.

Il tema della *governance* della blockchain è, quindi, fondamentale, poiché incide direttamente sulla fattibilità dei progetti in un dato ordinamento giuridico, tenuto altresì conto che l'essenza propria di tale tecnologia è proprio l'assenza di confini e, dunque, la possibilità di interagire con il diritto di ogni stato. A ciò si aggiunga che il GDPR si applica non solo ai soggetti con sede nell'Unione Europea, ma a tutte le organizzazioni che a vario titolo e a prescindere dalla loro collocazione geografica conservano dati personali relativi ai soggetti europei. Costituisce, dunque, un punto chiave la costruzione di una *governance* che miri a stabilire le regole di adesione, verifica e partecipazione, i ruoli, le responsabilità, le funzioni e i criteri decisionali. Nel tentativo di fornire una prima risposta alle questioni sopra illustrate, affrontando il problema dell'individuazione dei soggetti destinatari della legislazione privacy, non vi è dubbio che nelle blockchain del tipo consorzio o private, data la loro caratteristica strutturale,

⁷⁴ Per un esame di tali soluzioni si veda Fulvio Sarzana di S. Ippolito e Massimiliano Nicotra "Diritto della blockchain, intelligenza artificiale e IoT", Milano, 2018, p. 89.

⁷⁵ Peraltro, l'art. 17, al paragrafo 2,

precisa proprio che il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione.

porterebbe senz'altro ad individuare nel soggetto/i validatore/i del consenso il titolare del trattamento o il responsabile del trattamento, nei casi in cui questi gestisce il dato per conto del titolare. Diversa, invece, è la conclusione se si guarda la blockchain pubblica, caratterizzata da un contesto fortemente decentralizzato, nella quale sembra al quanto arduo identificare uno più soggetti che abbiamo un controllo sui dati registrati nel *ledger*.

Il dibattito su tali questioni è appena iniziato, e verte sul se il titolare del trattamento possa essere considerato lo stesso sviluppatore del protocollo ⁷⁶, o se siano gli stessi nodi che abbiano la capacità di esprimere il consenso, ma non sono coinvolti nel merito delle transazioni, o se siano gli utenti, o i programmatori degli *smart contracts*, i quali, peraltro, se coinvolti nell'elaborazione dei dati, potrebbero essere responsabili per gli errori nella loro esecuzione. Si pensi, inoltre, alla possibilità che i dati degli utenti si trovino in un paese al di fuori dell'UE immediatamente dopo la loro immissione, in violazione dell'art. 44 del GDPR che vieta il trasferimento dei dati all'estero a meno che non intervengano specifiche garanzie ⁷⁷. Se nelle blockchain private è possibile gestire e regolare tale aspetto, in quelle pubbliche regna l'assoluta indeterminazione del tempo e dello spazio.

Volendo trarre una prima conclusione, nelle fattispecie "pure" di blockchain, data la loro architettura completamente aperta, occorre guardare più che altro all'utente/nodo che immette i dati nella blockchain e il suo ruolo rispetto ai dati che gestisce. Detto nodo potrà, infatti, assumere la qualifica di titolare se determina le finalità e i mezzi del trattamento di dati personali ⁷⁸, o di responsabile se tratta, invece, i dati personali solo per conto del

⁷⁶ Lo sviluppatore dell'algoritmo può semplicemente essere un fornitore di soluzioni e, dunque, non partecipare al trattamento dei dati. Al contrario può invece elaborare dati per conto di un altro soggetto e, allora, in tal caso potrebbe assumere la qualifica di responsabile dei dati. Ad ogni modo, il GDPR impone l'adozione di misure tecniche ed organizzative adeguate al fine di tutelare i dati da trattamenti illeciti. L'art. 25, rubricato "Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita", paragrafi 1 e 2, in particolare, introduce il principio di *privacy by design* e *privacy by default*, un approccio concettuale innovativo che impone alle aziende l'obbligo di avviare un progetto prevedendo, fin da subito, gli strumenti e le corrette impostazioni a tutela dei dati personali.

⁷⁷ Ai sensi dell'art. 45 del GDPR infatti, "il trasferimento di dati personali verso

un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche". In assenza di una decisione di tale tipo, il trasferimento potrà avvenire solo in presenza di garanzie adeguate: a) strumento giuridicamente vincolante, avente efficacia tra autorità pubbliche o organismi pubblici; b) norme vincolanti d'impresa (*Binding corporate rules*); c) clausole tipo di protezione dei dati, adottate dalla Commissione; d) clausole tipo di protezione dei dati, adottate da un'autorità di controllo e approvate dalla Commissione; e) codice di condotta; f) meccanismo di certificazione; g) clausole contrattuali. (art. 46 GDPR).

⁷⁸ V. art. 4, par. 1, n. 7 GDPR.

titolare del trattamento ⁷⁹. A tale scopo occorre considerare che l'art. 2 del regolamento esclude la sua applicazione nel caso di trattamenti di dati personali effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un'attività commerciale o professionale. Inoltre, stante il carattere immutabile del contenuto dei blocchi della blockchain, problemi di compatibilità con il Regolamento sorgono in ordine al diritto alla cancellazione di quei dati che siano stati immessi nel sistema e dove nessuno ha né il potere né il diritto di manipolare o cancellare in tutto in parte ⁸⁰. L'utente, dunque, che si trovasse a operare in un tale sistema, nell'ottica di un principio di autoresponsabilità, dovrebbe aver valutato i rischi che tale tecnologia comporta e accettato le limitazioni ad alcuni diritti che, nel caso in esame, la regolamentazione sulla protezione dei dati gli attribuisce, in ragione della tecnica in uso in un dato momento storico.

3.1. Segue. *Il profilo dell'identità degli individui nel mondo virtuale e l'imputazione della volontà.*

Si è avuto modo di evidenziare come tale tecnologia oltre a innovare servizi già esistenti ⁸¹ consenta di creare nuovi servizi e modelli di business, sconosciuti al diritto e che necessitano di essere regolati a tutela degli interessi dell'individuo ⁸².

La regolamentazione dei nuovi contesti tecnologici in cui si estrinseca la personalità non potrà che richiedere uno sforzo di coordinamento tra i vari Paesi, stante la mancanza di confini territoriali con cui si manifestano le relazioni individuali più complesse. Come è stato per il commercio elettronico, vi è la presa d'atto dell'incapacità dei singoli ordinamenti nazionali di disciplinare il fenomeno economico entro i propri confini ⁸³.

I profili regolatori potranno riguardare, ad esempio, gli utenti della blockchain, imponendo loro diritti, obblighi e responsabilità

⁷⁹ V. art. 4, par. 1, n. 8 GDPR.

⁸⁰ Il CNIL nel documento citato (v. *supra*) rileva tuttavia che si potrebbe registrare una nuova transazione che annulli o rettifichi quella precedente. È pur vero che, in ogni caso, la transazione precedente continuerà ad apparire nella catena.

⁸¹ Si pensi all'utilizzo della blockchain per processare i pagamenti in tempo reale tra tutti gli intermediari (nodi) del *network*.

⁸² L'intelligenza artificiale, nell'*Internet of Things* e nell'analisi dei *big data*, permette oggi di progettare una tecnologia in grado di imparare a pensare sempre di più come le persone e di adattarsi ai loro desideri e bisogni, se non addirittura di

anticiparli. Sulle recenti applicazioni di soluzioni basate su sistemi di apprendimento automatico si v. G. CORASANITI, *Il diritto nella società digitale*, Milano, 2018.

⁸³ In aderenza al modello normativista di Hans KELSEN, Natalino IRTI, nel saggio *Norme e luoghi. Problemi di geo-diritto*, Roma-Bari 2001, evidenzia come la verità della norma va misurata alla luce della sua validità procedurale, che è disancorata dallo spazio, elemento esterno al diritto stesso. In tal modo, il diritto si fa duttile e sciolto "non ha paura degli spazi; è in grado di seguire la latitudine dell'economia. L'antitesi tra diritto territoriale ed economia planetaria cade col cadere stesso del fondamento tellurico" (p. 59).

o potrebbero essere imposti comportamenti per tutti i soggetti che forniscono la struttura tecnologica su cui sono implementate le blockchain. L'Italia, con il d.lgs. 25 maggio 2017, n. 90, recante modifiche alla normativa italiana in materia di antiriciclaggio e contrasto al finanziamento del terrorismo⁸⁴, anticipando l'orientamento del legislatore comunitario⁸⁵, è già intervenuta sul tema dell'adeguata verifica della clientela inserendo a pieno titolo tra i soggetti obbligati, quali "altri operatori non finanziari", i prestatori di servizi relativi all'utilizzo di moneta virtuale⁸⁶. Con tali disposizioni si è sostanzialmente voluto intercettare i punti di snodo principali in ordine all'accesso ed alla fuoriuscita dalle blockchain delle criptovalute⁸⁷, limitando in parte — ma non del tutto — il carattere di pseudo anonimato che contraddistingue tali sistemi⁸⁸.

Il dibattito è in pieno svolgimento. In sede europea, *de iure condendo* il Parlamento, con una recente risoluzione⁸⁹, ha invitato la Commissione a collaborare con gli Stati membri in modo da

⁸⁴ Il d.lgs. n. 90/2017, in vigore dal 4-7-2017, dando attuazione alla delega contenuta nella legge 12 agosto 2016, n. 170 e modificando il d.lgs. n. 231/2007, ha recepito la Direttiva del Parlamento Europeo e del Consiglio 849/2015 del 20-5-2015 (c.d. IV Direttiva antiriciclaggio), che integra ed abroga le dir. 2005/60/CE e 2006/70/CE e applica le raccomandazioni GAFI, come revisionate da ultimo nel febbraio 2012.

⁸⁵ Il 19 giugno 2018 è stata pubblicata nella Gazzetta Ufficiale UE la direttiva n. 2018/843 del Parlamento europeo e del Consiglio, del 30 maggio 2018 (cosiddetta V direttiva antiriciclaggio), che modifica la direttiva 2015/849 (IV direttiva antiriciclaggio), recepita in Italia già recepita in Italia dal d.lgs. n. 90/2017.

⁸⁶ I soggetti in questione sono definiti quali "ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, servizi funzionali all'utilizzo, allo scambio alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale" (art. 1, co. 2, lett. ff), ed il perimetro è riferito "limitatamente allo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso" (art. 3, co. 5, lett. i). In tale definizione sembrerebbero rientrare anche i c.d. *wallet provider*, ossia coloro i quali offrono servizi di custodia delle credenziali necessarie per accedere alle valute virtuali.

⁸⁷ Le valute virtuali, secondo la definizione riportata nel d.lgs. n. 231/2007, sono la rappresentazione digitale di valore, non emesse da una Banca centrale o da un'autorità pubblica, non necessariamente colle-

gate ad una valuta avente corso legale, utilizzate come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente.

⁸⁸ Si veda la sentenza del Tribunale di Verona (Trb. Verona, 24 gennaio 2017, in *Banca Borsa Titoli di Credito* 2017, 4, II, 467, con nota di Passaretta) primo *leading case* italiano in un'operazione di *crowdfunding* in bitcoin, nel quale il tribunale ha ritenuto di applicare gli obblighi di informativa di natura precontrattuale dettati dal perimetro normativo tracciato dagli artt. 67 *quater*, *quinquies*, *sexies*, *septies*, *decies* ed *undecies*, del Codice del Consumo, così come integrato in via regolamentare (*ex art.* 67 *decies*) dal Titolo III dell'Allegato 1 della delibera Consob n. 18592 del 26 giugno 2013 (Regole di condotta: artt. 13-21). Per un commento si rinvia a M. GIULIANO, "L'adempimento delle obbligazioni pecuniarie nell'era digitale. Dalla moneta legale alla moneta scritturale e digitale "legalmente" imposta", Torino, 2018, p. 165.

⁸⁹ I 23 paesi europei hanno deciso di dare vita alla European Blockchain Partnership, alla quale, recentemente, ha aderito anche l'Italia, una iniziativa che punta a favorire la collaborazione tra gli stati membri per lo scambio di esperienze e di *expertise*, sia sul piano tecnico sia su quello della regolamentazione. In sede europea, il Commissario per l'economia e la società digitale, Mariya Gabriel, ha peraltro osservato che tutti i servizi pubblici in futuro potranno utilizzare la tecnologia blockchain nell'ottica di ripensamento dei sistemi informativi, per disporre di soluzioni che per-

sviluppare un ambiente normativo favorevole all'innovazione, tale da rimuovere le barriere esistenti alla creazione delle strutture di blockchain, promuovendo al contempo l'armonizzazione all'interno dell'Unione e valutando l'idea di introdurre un passaporto europeo di progetti basati sulle DLT. La Risoluzione sottolinea, tra l'altro, come i contratti intelligenti siano un elemento importante abilitato dalle DLT e possono fungere da fattori chiave delle applicazioni decentralizzate. Purtuttavia, il legislatore europeo evidenzia la necessità che la Commissione effettui una valutazione approfondita delle potenzialità e delle implicazioni giuridiche, ad esempio i rischi relativi alla giurisdizione. Vengono, inoltre, rimarcate le potenzialità della firma digitale crittografata per favorire gli *smart contracts*. Per quanto attiene la proprietà intellettuale, nel caso dei contenuti creativi "digitalizzati", le DLT possono consentire di tracciare e gestire la proprietà intellettuale e facilitare la protezione dei diritti d'autore e dei brevetti.

Dal punto di vista del diritto positivo, negli Stati Uniti ⁹⁰ riscontriamo già alcuni stati che hanno emanato norme specifiche che attribuiscono validità giuridica alle componenti di una blockchain o di una DLT, come nel caso, solo per citarne alcuni, dello Stato del Tennessee, della California ⁹¹ e dell'Arizona. In via generale si attribuisce valore legale alla tecnologia blockchain e agli *smart contracts* nella conduzione di transazioni elettroniche, ricono-

mettano di aumentare la fiducia dei cittadini e di garantire sempre meglio la protezione dei dati personali. Il 3 ottobre 2018 il Parlamento Europeo ha peraltro approvato la risoluzione P8_TA-PROV(2018)0373 dal titolo "Tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione" con la quale, premettendo, tra l'altro, che le tecnologie di registro distribuito (DLT) e blockchain possono costituire uno strumento che rafforza l'autonomia dei cittadini dando loro l'opportunità di controllare i propri dati e decidere quali condividere nel registro, e migliorare l'efficienza dei costi delle transazioni eliminando intermediari e costi di intermediazione, analizza le possibili applicazioni nei diversi settori dell'industria e dei servizi, quale quello dei trasporti, sanitario, finanziario e nelle catene di approvvigionamento. La risoluzione interviene anche in ordine ai contratti intelligenti, c.d. *smart contract*, sottolineando la loro importanza chiave nell'ambito delle applicazioni decentralizzate. Il Parlamento, tuttavia, invita la Commissione ad effettuare una valutazione approfondita delle potenzialità e delle implicazioni giuridiche, quali quelle legate ai rischi

relativi alla giurisdizione o alla validità di una firma digitale crittografata, requisito indispensabile per assicurare la certezza del diritto. Inoltre, quanto al nostro ordinamento, nel decreto semplificazioni approvato lo scorso 16 ottobre 2018 dal Consiglio dei Ministri, insieme al decreto fiscale 2019 e alla manovra economica, sono peraltro previste misure a favore della blockchain, dove si stabilisce che tale tecnologia ha "la stessa validità giuridica attribuita a informazioni e dati certificati attraverso l'uso di altre tecnologie". La relazione illustrativa al decreto fa alcuni esempi di possibili applicazioni nel pubblico: passaporti e certificati anagrafici, registri (aziendali, scolastico), riscossione imposte, gestione di identità digitali. Nel privato gli esempi citati riguardano *smart contract*, tracciabilità di transazioni, contrasto alla contraffazione del *made in Italy*.

⁹⁰ <http://www.ncsl.org/research/financial-services-and-commerce/the-fundamentals-of-risk-management-and-insurance-viewed-through-the-lens-of-emerging-technology-webinar.aspx>.

⁹¹ http://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB2658.

scendo i diritti di proprietà di determinate informazioni garantite dalla blockchain, per cui non può essere negato l'effetto giuridico, la validità o l'esecutività di una transazione solo perché avvenuta per il tramite di tali tecnologie. Il Governo italiano, dopo un primo tentativo, poi naufragato, attraverso il decreto legge 14 dicembre 2018 n. 135, G.U. 14 dicembre 2018, di semplificazione per le imprese e per la pubblica amministrazione, ha nuovamente presentato un emendamento al predetto decreto, nella fase di conversione, inserendo una norma che dal un lato definisce le tecnologie basate su registri distribuiti, le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, 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; e dall'altro stabilisce che la memorizzazione di un documento informatico attraverso l'uso delle DLT produce gli effetti giuridici della validazione temporale elettronica di cui all'art. 41 del Regolamento UE n. 910/2014⁹².

De iure condito, alla luce della normativa e delle categorie vigenti, la tecnologia blockchain, al momento, potrà senz'altro giovare del Regolamento eIDAS (*Electronic Identification Authentication and Signature*) n. 910/2014/UE del Parlamento Europeo e del Consiglio del 23 luglio 2014⁹³ e del d.lgs. 82/2005, Codice dell'Amministrazione Digitale o CAD⁹⁴.

Difatti, i dati registrati nella blockchain possono senz'altro

⁹² L'art. 41, rubricato "Effetti giuridici della validazione temporale elettronica" stabilisce: "1. Alla validazione temporanea elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziari per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti della validazione temporanea elettronica qualificata. 2. Una validazione temporale elettronica qualificata gode della presunzione di accuratezza della data e dell'ora che indica e di integrità dei dati ai quali tale data e ora sono associate. 3. Una validazione temporale elettronica rilasciata in uno Stato membro è riconosciuta quale validazione temporale elettronica qualificata in tutti gli Stati membri".

⁹³ Il Regolamento disciplina la "identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno" ed è entrato in vigore il 17 settembre 2014 ma si applica, nelle sue parti operative, dal 1 luglio 2016. Da tale data la Direttiva 1999/93/CE del 13 dicembre 1999

relativa alla disciplina delle firme elettroniche, è abrogata. Il Regolamento, partendo da un approccio di neutralità dal punto di vista della soluzione tecnologica da adottare riguardo ai sistemi di gestione dell'identità elettronica e relative infrastrutture, si pone l'obiettivo di rafforzare la fiducia nelle transazioni nell'Unione Europea, fornendo una base normativa comune per interazioni elettroniche sicure fra cittadini, imprese e pubbliche amministrazioni. Ha inoltre eliminato le barriere esistenti all'impiego transfrontaliero dei mezzi di identificazione elettronica utilizzati negli Stati membri, al fine di garantire che per accedere ai servizi online transfrontalieri offerti dagli Stati membri si possa disporre di un'identificazione e un'autenticazione elettronica sicura.

⁹⁴ Il CAD è stato di recente modificato dal d.lgs. 179/2016, che ha inteso armonizzare le disposizioni nazionali al mutato quadro normativo europeo, e dal regolamento comunitario n. 910/2014 (c.d. Regolamento eIDAS), al quale il CAD opera un rinvio diretto quanto alle definizioni, abrogando

considerarsi alla stregua di un “documento informatico” in base alle disposizioni del CAD ⁹⁵, che lo definiscono come la “rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti” o anche alla stregua di un “documento elettronico” ai sensi del regolamento, definito come “qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva” ⁹⁶. Più problematico è, invece, l’aspetto della riconducibilità di un dato documento informatico al soggetto che lo ha creato.

Sotto questo aspetto, il Regolamento e il CAD, quali metodi di identificazione informatica e di certificazione della titolarità di documento informatico, prevedono quattro diverse tipologie di firme, le prime tre disciplinate nel Regolamento (la firma elettronica, elettronica avanzata, elettronica qualificata) ⁹⁷ e la quarta, la firma digitale, nel CAD. In dettaglio, la firma elettronica “semplice” rappresenta la più semplice fattispecie di sottoscrizione informatica. È costituita dall’insieme “dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica. Un esempio di firma elettronica cd. semplice è dato dall’utilizzo di *User Id* e di una *password* che consentono ad un soggetto di accedere ad un servizio.

La firma elettronica avanzata è, invece, l’insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consente l’identificazione del firmatario del documento e garantisce la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo. Un esempio di tale tipo di firma è la firma grafometrica, che consiste in quella firma autografa apposta con un pennino, su una tavoletta elettronica, conferendo una certezza elevatissima in merito alla riconducibilità di quella firma alla nostra persona ⁹⁸. La firma elettronica qualificata è, invece, definita un particolare tipo

quelle precedentemente previste in esso. Inoltre, la disciplina introdotta dal CAD è stata integrata dalle regole tecniche di cui al D.P.C.M. 30 marzo 2009, al D.P.C.M. 22 febbraio 2013 e da ultimo al D.P.C.M. 13 novembre 2014, integrazioni che garantiscono nel tempo l’adeguamento del CAD all’evoluzione tecnologica rispetto agli standard a livello internazionale. Da ultimo, è intervenuto il d.lgs. 13 dicembre 2017, n. 217, “Disposizioni integrative e correttive al decreto legislativo 26 agosto 2016, n. 179, concernente modifiche ed integrazioni al Codice dell’amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell’articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche”.

⁹⁵ Art. 1, lett. p, CAD.

⁹⁶ Il Considerando n. 63 chiarisce che a un documento elettronico non dovrebbero essere negati gli effetti giuridici per il motivo della sua forma elettronica e, ai sensi dell’art. 46, l’ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica.

⁹⁷ Reg., art. 3, nn. 10-12.

⁹⁸ Nella firma grafometrica si costituisce un *set* di informazioni biometriche che, con l’ausilio di tecniche crittografiche, viene strettamente associato a un determinato documento informatico, in modo tale da consentire *ex post* lo svolgimento di analisi grafologiche da parte di un perito calligrafo sulla genuinità della “sottoscrizione”. Rispetto ad altri dati biometrici (definiti nel

di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma. Infine, la firma digitale, definita nel CAD, è, invece, un particolare tipo di firma qualificata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici. Quindi, la firma digitale rientra nel novero delle firme elettroniche qualificate che, a propria volta, rappresentano una tipologia di firma elettronica avanzata. La firma elettronica qualificata (e quindi anche la firma digitale che ne costituisce a tutti gli effetti una *species*) rispetto alla semplice firma elettronica avanzata avrà due ulteriori caratteristiche fondamentali (si veda art. 25 Reg. eIDAS): *a*) gode del medesimo valore giuridico attribuito ad una firma autografa; *b*) qualora sia basata su di un certificato qualificato rilasciato in uno Stato membro dell'Unione Europea, sarà pienamente riconosciuta in tutti gli Stati di detta Unione.

Alle firme elettroniche sopra esposte, il CAD, a seguito della modifica intervenuta con il d.lgs. 13 dicembre 2017, n. 217, ha introdotto una nuova modalità di creazione di documenti informatici con efficacia probatoria di cui all'art. 2702 c.c., pari a quelli sottoscritti con firma digitale, qualificata o avanzata, qualora rispetti gli standard tecnici individuati dall'AgID⁹⁹, mentre, nei restanti casi, il valore probatorio del documento informatico è rimesso al libero giudizio degli organi giudicanti¹⁰⁰.

Ebbene, si è visto che il processo di “firma” delle informazioni

GDPR, art. 4 come dati personali, ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca) la firma grafometrica presenta delle peculiarità che la rendono meno affidabile (a causa della sua instabilità nel tempo e dei suoi elevati tassi di falsi negativi) nei sistemi di autenticazione ed identificazione biometrica, ma al contempo più efficace nelle procedure di sottoscrizione di documenti, soprattutto perché la sua rilevazione richiede la partecipazione attiva del firmatario.

⁹⁹ L'Agenzia per l'Italia digitale (abbreviato AgID) è una agenzia pubblica italiana istituita con il decreto legge 22 giugno 2012 n. 83 (cosiddetto “Decreto sviluppo”) convertito in legge 7 agosto 2012 n. 134. Svolge le funzioni ed i compiti ad essa attribuiti dalla legge al fine di perseguire il

massimo livello di innovazione tecnologica nell'organizzazione e nello sviluppo della pubblica amministrazione e al servizio dei cittadini e delle imprese, nel rispetto dei principi di legalità, imparzialità e trasparenza e secondo criteri di efficienza, economicità ed efficacia.

¹⁰⁰ A seguito del completamento della procedura di notifica del Sistema Pubblico di Identità Digitale (SPID), ultimato dall'Agenzia con la pubblicazione nella Gazzetta Ufficiale dell'Unione Europea (GUUE C318 e GUUE C344 del 2018), a decorrere dal 10 settembre 2019 l'identità digitale SPID potrà essere usata per l'accesso ai servizi in rete di tutte le pubbliche amministrazioni dell'Unione. Questo diritto, introdotto dal regolamento eIDAS, potrà essere anticipato dagli Stati membri che potranno decidere se consentire l'accesso anche ai propri servizi che prevedono l'uso di credenziali di livello 1. Per l'accesso a servizi che preve-

scambiate nella blockchain è proprio quello previsto dalla crittografia in uso nella firma digitale, definita di tipo asimmetrico o a chiave pubblica ¹⁰¹. La differenza sostanziale tra i due sistemi è che in un sistema regolamentato, come quello disciplinato dal Regolamento e dal CAD, vi è un processo preliminare di certificazione che consente di avere l'effettiva certezza dell'identità del titolare della coppia di chiavi ¹⁰². Abbiamo, infatti, visto come nel sistema Bitcoin chiunque possa ottenere una coppia di chiavi, privata e pubblica, per scambiare criptovaluta senza la necessità di doversi identificare ¹⁰³.

La firma digitale, dunque, rappresenta l'esito di un processo tecnologico-giuridico, che si fonda su una precisa scelta tecnologica (utilizzo della crittografia asimmetrica) e giuridica, per cui il documento informatico sottoscritto con firma digitale (o firma elettronica avanzata o qualificata), formato nel rispetto delle regole tecniche di cui all'art. 20, comma 3 ¹⁰⁴, ha valore di piena prova ex art. 2702 c.c.

dono l'uso di credenziali di livello 2 e 3, è prevista l'obbligatorietà di consentire l'accesso con le credenziali SPID di pari livello. (V. <https://www.agid.gov.it/it/piattaforme/spid>).

¹⁰¹ Il legislatore già nel Decreto del Presidente della Repubblica 10 novembre 1997, n. 513 (Regolamento contenente i criteri e le modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59), abrogato dal D.P.R. 445/2000 (Testo Unico in materia di documentazione amministrativa), definiva all'art. 1, lett. d), le chiavi asimmetriche come la coppia di chiavi crittografiche, una privata ed una pubblica, correlate tra loro, da utilizzarsi nell'ambito dei sistemi di validazione o di cifratura di documenti informatici; alla lett. e), la chiave privata, l'elemento della coppia di chiavi asimmetriche, destinato ad essere conosciuto soltanto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico o si decifra il documento informatico in precedenza cifrato mediante la corrispondente chiave pubblica; alla lett. f) la chiave pubblica, l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche o si cifrano i documenti informatici da trasmettere al titolare delle predette chiavi.

¹⁰² La firma digitale è richiesta presso il certificatore (Certification Authority, detto anche CA) o TTP (*Trusted Third Part*) o

Terza Parte Fidata (TPF), il quale, previa identificazione e registrazione del richiedente, rilascerà il *kit* per la firma, consistente, il più delle volte, in un lettore di *smart card* con collegamento USB o *token* USB che consentono di usare *smart card* in formato SIM, un *software* e un dispositivo di firma nonché un codice identificativo univoco per la connessione sicura con il certificatore. Una volta generate le chiavi l'utente dovrà inviare quella pubblica al certificatore, il quale, effettuare le dovute verifiche in ordine all'unicità della chiave stessa, procederà alla emissione e pubblicazione del certificato. Il certificatore che rilascia certificati di firma elettronica qualificata o digitale e i certificati della chiave pubblica, curandone la pubblicazione aggiornata degli elenchi, assume la denominazione di "prestatore di servizio fiduciario qualificato", in forza di un riconoscimento da parte dell'organismo di vigilanza, nel rispetto dei requisiti dettati dall'art. 24 del regolamento eIDAS.

¹⁰³ A mero titolo esemplificativo, fra i sistemi di crittografia maggiormente utilizzati che sfruttano la tecnica della chiave pubblica e privata, che chiunque può creare senza necessità di alcuna identificazione, si cita il software denominato *Pretty Good Privacy* (PGP). V. M. MARTONI, *Temì di diritto dell'informatica*, AA.VV., a cura di Claudio di Cocco e Giovanni Sartor, Torino, 2017 p. 47.

¹⁰⁴ Tale norma statuisce che alla base della firma elettronica (qualificata o digitale) vi sia un certificato non scaduto, non revocato e non sospeso.

La blockchain, dunque, seppur utilizza componenti tecnologiche proprie della firma digitale regolamentata, tuttavia non soddisfa i principi normativi comunitari stabiliti nel Regolamento eIDAS e nel CAD in ordine alla certificazione dell'identità sottostante le chiavi crittografiche e alla validazione temporali elettroniche. Con riferimento a tale ultimo aspetto le marche temporali (*timestamp*) sono un servizio offerto da un Certificatore accreditato, che consente di associare data e ora, certe e legalmente valide, ad un documento elettronico, permettendo una validazione temporale del documento opponibile a terzi ¹⁰⁵. Nel caso della blockchain le marche temporali non sono emesse da un Prestatore di Servizi Fiduciari come previsto nel Regolamento eIDAS, ma ciascun blocco contiene un riferimento temporale non particolarmente accurato ¹⁰⁶.

Il ceto notarile ha, tuttavia, avuto modo di evidenziare “le potenzialità devastanti” della piena fungibilità della sottoscrizione digitale, che impieghi strumenti di identificazione e tecnologia blockchain che fanno a meno di un'autorità terza, quale figura garante della certezza dei traffici giuridici.

Pur nella consapevolezza della necessità di un “certificatore” all'origine del processo di creazione di un'identità digitale, l'attuale quadro giuridico, poc'anzi sinteticamente illustrato, consentirebbe di fornire validità giuridica alle transazioni virtuali processate in un ambiente virtuale — naturalmente scollegato dall'ambiente “reale” —, allo stesso modo in cui sono valide giuridicamente quelle che si compiono dinanzi al notaio, terzo garante e sul quale riporre fiducia. È pur vero che esiste sempre un margine di incertezza dettato dalla impossibilità di avere la certezza che chi ha utilizzato una firma digitale in un dato momento sia anche il titolare della stessa. Una certezza che si potrà ottenere probabilmente solo con le firme grafometriche o biometriche, magari combinate con le altre firme elettroniche o certificazioni.

Una recente sentenza del Tribunale di Roma, depositata il 23 gennaio 2017, mette in evidenza proprio l'aspetto debole della firma digitale, che certamente non assicura che sia stato proprio

¹⁰⁵ Cfr. Art. 20, comma 3 CAD. Il regolamento europeo eIDAS introduce due definizioni: validazione temporale elettronica, vale a dire dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento; validazione temporale elettronica qualificata, ovvero una validazione temporale elettronica che soddisfa i requisiti di cui all'articolo 42 del regolamento eIDAS. In particolare, la validazione temporale qua-

lificata prevede l'apposizione della marca temporale mediante una firma elettronica avanzata o sigillata con un sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato o mediante un metodo equivalente.

¹⁰⁶ V. G. MANCA, *Blockchain e firma elettronica, normative a confronto*, in *Agenda Digitale*, <https://www.agenda-digitale.eu/documenti/blockchain-e-firma-elettronica-normativa-a-confronto-analogie-e-differenze/>, sito consultato il 30.10.2018.

il titolare ad utilizzare e ad autorizzare la transazione o sottoscrivere un atto.

Il tribunale capitolino 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. Il Tribunale ha ritenuto, dunque, applicabile l'art. 21, comma 2, CAD secondo cui in relazione al tipo di documento (informatico) e di firma (digitale), l'uso del dispositivo si presume riconducibile al titolare, salvo che questi dia 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 digitale. Il caso deciso dal tribunale è, tuttavia, un caso limite, poiché nel caso di specie è mancato proprio il controllo sulla genuinità della firma apposta sull'atto da parte del commercialista-intermediario incaricato di trasmettere l'atto al registro delle imprese¹⁰⁷, che ha viziato l'intero procedimento volto ad apporre la firma digitale sul documento informatico. Infatti, la firma digitale diviene requisito di forma quando il procedimento di trasferimento di partecipazioni societarie è quello di cui all'art. 36, comma 1-bis e il documento sottoscritto con firma digitale soddisfa il requisito legale della forma scritta se formato nel rispetto delle regole

¹⁰⁷ Il decreto legge 112/2008, convertito, con modificazioni, in legge n. 133 del 6 agosto 2008, ha introdotto novità in tema di trasferimento di partecipazioni in società a responsabilità limitata. In particolare, ci si riferisce all'articolo 36, comma 1-bis che così recita: "L'atto di trasferimento di cui al secondo comma dell'articolo 2470 del codice civile può essere sottoscritto con firma digitale, nel rispetto della normativa anche regolamentare concernente la sottoscrizione dei documenti informatici, ed è depositato, entro trenta giorni, presso l'ufficio del registro delle imprese nella cui circoscrizione è stabilita la sede sociale, a cura di un intermediario abilitato ai sensi dell'articolo 31, comma 2-quater, della legge 24 novembre 2000, n. 340. In tale caso, l'iscrizione del trasferimento nel libro dei soci ha

luogo, su richiesta dell'alienante e dell'acquirente, dietro esibizione del titolo da cui risultino il trasferimento e l'avvenuto deposito, rilasciato dall'intermediario che vi ha provveduto ai sensi del presente comma. Resta salva la disciplina tributaria applicabile agli atti di cui al presente comma". In conseguenza di tale modifica, il contratto avente a oggetto la cessione delle quote di partecipazione al capitale di una Srl può essere pubblicato nel Registro imprese anche se « sottoscritto con firma digitale » non autenticata. Questi atti possono essere trasmessi al Registro imprese solo dagli intermediari a ciò abilitati (e cioè dagli iscritti negli albi dei dottori commercialisti, dei ragionieri e periti commerciali). Oltre all'adempimento al registro imprese gli intermediari, entro 20 giorni dalla stipula, effettuano la registrazione presso l'agenzia delle Entrate.

tecniche che, ai sensi dell'art. 71 CAD, garantiscono l'identificazione dell'autore e l'integrità del documento medesimo¹⁰⁸.

Peraltro, la possibilità di fornire una prova contraria implica la possibilità di addivenire ad un accertamento circa l'utilizzo del dispositivo di firma da parte di un soggetto diverso dal titolare. Si tratta, a ben vedere, di uno strumento di tutela che viene fornito al soggetto che lamenti un utilizzo fraudolento della propria firma, in assenza del quale avrebbe maggiori difficoltà a procurarsi la prova dell'autenticità del documento, poiché, come è ovvio, non bisognerà andare a verificare l'effettiva corrispondenza del segno grafico a quello apposto in precedenza, ma, altresì, bisognerà verificare se è stata garantita e se è provato l'utilizzo esclusivo del dispositivo di firma.

Ciò posto, dunque, si concorda con quella parte della dottrina che ritiene che con le cosiddette "firme" elettroniche o digitali si è passati da un modello basato sull'autorialità ad un modello basato sulla responsabilità¹⁰⁹ 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 provoca e agli affidamenti che ingenera. È tuttavia, innegabile che, sebbene quanto agli effetti, la firma digitale è equiparata alla sottoscrizione autografa, tuttavia la natura delle due forme di attribuzione della paternità di un documento ad un soggetto sono ontologicamente diverse: "apposizione olografa da parte dall'autore del documento del proprio nome e cognome" e "sequenza crittografica di byte volta a costituire il segno personale di chi la appone"¹¹⁰.

4. DAL CONTRATTO CIBERNETICO ALLO SMART CONTRACT.

La blockchain è stata paragonata a Internet nei primi anni '90: mentre Internet ha trasformato il modo in cui condividiamo le informazioni e ci connettiamo, la blockchain, detta anche *Internet of value*, sta trasformando il modo in cui scambiamo valore e di cui ci fidiamo. Inizialmente ha trovato applicazione nei pagamenti, consentendo il trasferimento di bitcoin tra due soggetti, senza la necessità di un intermediario, ha poi esteso lo spettro di

¹⁰⁸ Sulle verifiche che l'intermediario deve effettuare si rinvia alla circolare n. 6/IR del 22 ottobre 2008 emanata dal Consiglio nazionale dei dottori commercialisti e degli esperti contabili.

¹⁰⁹ G. FINOCCHIARO, *Il contratto nell'era dell'intelligenza artificiale*, in *Riv. Trim. di Dir. e Proc. Civ.*, fasc. 2, 2018, p. 441. L'Autore richiama peraltro il parere del Consiglio di Stato del 7 febbraio 2005, n. 11995 sul Codice dell'Amministrazione Di-

gitale, il quale in materia di disconoscimento afferma che "sembra giusto superare i vecchi concetti di falso, strettamente legati al principio di "paternità" della firma e non a quello di "responsabilità" per la firma; dall'altro occorre fare assoluta chiarezza sulle ipotesi in cui è consentito dimostrare l'assenza di responsabilità".

¹¹⁰ Cass., 10 novembre 2015, n. 22871, in *Ilprocessotelematico.it*, 2015, con nota di Forner Emanuele.

applicazioni, essendo idonea, utilizzando una criptovaluta, a certificare digitalmente contratti, dichiarazioni sottostanti e dati relativi all'identità delle parti. Inoltre, grazie all'utilizzo di ulteriori codici informatici, la blockchain è diventata anche finanche "luogo" dove sorgono gli accordi.

Ed è proprio sul fronte dei contratti "smart", che la blockchain sembra aprire nuovi orizzonti. Gli *smart contracts*¹¹¹ hanno radici piuttosto lontane, ma solo con l'avvento della tecnologia blockchain hanno trovato il terreno giusto per germogliare ed esprimere tutto il loro valore aggiunto, grazie a quelle garanzie di fiducia, affidabilità e sicurezza proprie della blockchain, che, prima del suo avvento, erano riposte in una figura terza o nella spontanea esecuzione della controparte. Si deve a Nick Szabo la base di sviluppo del sistema di *smart contracts*, che prese forma per la prima volta nel 1997 nei due suoi *papers*, *Formalizing and Securing Relationships on Public Networks*¹¹² e *The Idea of Smart Contracts*¹¹³, in cui l'autore prendeva spunto dal sistema di vendita dei distributori automatici per teorizzare il trasferimento di alcuni diritti in esecuzione di un algoritmo. In conseguenza dell'inserimento della quantità di moneta richiesta per lo specifico prodotto scelto, chiunque può effettuare uno scambio con il venditore, con il quale — in effetti — stipula un contratto. Szabo sostiene che è possibile attivare alcune clausole direttamente nel *software*, in maniera da rendere l'inadempimento scarsamente conveniente, se non addirittura proibitivo, in termini economici¹¹⁴.

Un contratto intelligente ha uno schema piuttosto semplice, poiché non è altro che la trasposizione di clausole contrattuali in un codice informaticamente eseguibile e inserite in un registro logico, per cui al verificarsi di una certa condizione, matematicamente accertabile, si produce l'evento digitalmente collegato¹¹⁵; funzionano con una logica "if this then that" ossia, al verificarsi

¹¹¹ M. RASKIN, *The law and legality of smart contracts*, in *Georgetown Law Technology Review*, Vol. 1:2, 2017, p. 305, il quale definisce uno *smart contract* "an agreement whose execution is automated". Kunnapas, *From Bitcoin to Smart Contracts: Legal Revolution or Evolution from the Perspective of de lege ferenda*, in Kerikmäe-Rull (eds), *The Future of Law and eTechnologies*, Springer, 2016; D. DI SABATO, *Gli smart contracts: robot che gestiscono il rischio contrattuale*, in *Contratto impresa*, 2017, p. 378 ss.; P. CUCCURU, *Blockchain e automazione contrattuale. Riflessioni sugli smart contracts*, in *Nuova giur. civ. comm.*, 2017, p. 107.

¹¹² Nick SZABO, *Formalizing and Secu-*

ring Relationships on Public Networks, 1997, <https://journals.uic.edu/ojs/index.php/fm/article/view/548/469#introduction>.

¹¹³ Nick SZABO, *The Idea of Smart Contracts*, 1997, <http://szabo.best.vwh.net/idea.html>.

¹¹⁴ Nel 1998 Szabo formalizzava in un terzo lavoro i concetti già individuati nei due precedenti scritti. Si v. N. SZABO, *Secure Property Titles with Owner Authority*, 1998, <http://szabo.best.vwh.net/securetitle.html>.

¹¹⁵ Si pensi all'ipotesi di un'auto munita di un programma che blocca automaticamente l'accensione nel caso in cui non vengano saldate le rate del finanziamento contratto per il suo acquisto.

delle circostanze dedotte allora si avrà un'azione automatizzata¹¹⁶.

Si è detto che gli *smart contracts* hanno acquisito rilevanza con l'avvento della blockchain, grazie alla possibilità di garantire l'esecuzione del contratto indipendentemente dal volere delle parti coinvolte nel contratto. Si tratta di una nuova modalità di manifestazione del consenso, che si aggiunge a quella del contratto telematico e a quella del contratto c.d. cibernetico¹¹⁷, caratterizzato, tale ultima tipologia, dall'ulteriore elemento dell'automazione delle istruzioni date tramite appositi *software* (c.d. *software agents* o *bot*)¹¹⁸, che consentano, al verificarsi di determinate condizioni, di assolvere il compito di decidere se, quando, con chi ed a quali condizioni stipulare un contratto in nome e per conto della parte. Lo *smart contract* si pone, a ben vedere, come un'evoluzione del contratto cibernetico, nel momento in cui è eseguito in una blockchain. Difatti, mentre nel contratto telematico l'uso del computer costituisce mezzo di telecomunicazione per trasmettere la proposta di un contratto e riceverne l'accettazione, in adesione a quanto già concordato dalle parti, nel contratto cibernetico, invece, è lo stesso contenuto del contratto ad essere lasciato alle determinazioni del computer, sebbene entro le istruzioni del *software* volute dalle parti stesse, nello *smart contract* è la tecnologia blockchain che caratterizza ulteriormente il con-

¹¹⁶ Ad esempio *IF* Tizio ha contratto una obbligazione con Caio *AND IF* l'obbligazione è scaduta *THEN* l'obbligazione è esigibile.

¹¹⁷ R. BORRUSO, S. RUSSO, C. TIBERI, *L'informatica per il giurista. Dal Bit a internet*, Milano, 2006, p. 347.

¹¹⁸ Il concetto di agente *software* è nato all'inizio degli anni '80, come punto d'incontro tra il campo di ricerca dell'intelligenza artificiale e quello dell'informatica; il suo scopo era fornire una soluzione che permettesse di risolvere, in maniera automatizzata, i problemi che l'espansione delle reti di calcolatori (*Internet in primis*) iniziava a porre. Si tratta di "applicativi che, sfruttando l'intelligenza artificiale, agiscono secondo schemi operativi che replicano, in senso lato, il modello della rappresentanza. In altre parole, i software in questione agiscono, sotto il profilo tecnico-informatico e socio-relazionale, come fossero dei "rappresentanti" (*agent*) dell'utente, stabilendo con un certo grado di autonomia se stipulare o meno il contratto, a quali condizioni e con quali contenuti (in questo senso F. Bravo, *Contratto cibernetico*, Dir. informatica, fasc.2, 2011, pag. 169). Senza poter entrare nel merito della disputa in ordine alla na-

tura giuridica dei *software agents*, basti qui rilevare che la "*Guide to Enactment*" che accompagna la UNCITRAL Model Law on Electronic Commerce, stabilisce che "The Data messages that are generated automatically by computers without human intervention should be regarded as "originating" from the legal entity on behalf of which the computer is operated". In questa prospettiva gli agenti non sono che meri strumenti di comunicazione e si riconosce natura contrattuale alle operazioni negoziali poste in essere tramite l'interazione tra e con sistemi elettronici di negoziazione automatica, senza l'intervento umano. Si veda anche la Convenzione UNCITRAL sull'e-contracting (United Nations Convention on the Use of Electronic Communications in International Contracts) dove all'art. 12, "Use of automated message systems for contract formation", si afferma che "A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, shall not be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems or the resulting contract".

tratto cibernetico, grazie alla completa disintermediazione dal fattore umano.

In altre parole, sia il contratto cibernetico che lo *smart contract* sono caratterizzati dal fatto che il computer/il codice informatico/l'algoritmo sono il mezzo di formazione genetica o integrazione della volontà contrattuale delle parti del rapporto.

Infatti, nel classico rapporto contrattuale e nelle altre tipologie contrattuali, ciascuna parte, seppur vincolata dalle obbligazioni contratte verso l'altra parte, resta comunque libera, con diversa ampiezza, di non dare seguito a quanto pattuito se disposto a sopportare le conseguenze di un inadempimento. Questa facoltà di scelta non è, invece, lasciata dalla blockchain, poiché lo *smart contract*, una volta lanciato nella rete, è immodificabile e segue esclusivamente le istruzioni programmate. Ciò a meno che non si intervenga, dal punto di vista tecnico, con una istruzione contraria a quella in precedenza impartita. Aspetto, quest'ultimo, che è da analizzare, la cui fattibilità è legata al tipo di blockchain nella quale il codice informativo è eseguito ¹¹⁹. È evidente il vantaggio di un tale meccanismo, poiché colui che ha ceduto un bene si vedrà accreditare il prezzo pattuito non appena il sistema informatico avrà registrato la consegna del bene. Ogni contestazione potrà sicuramente trovare spazio successivamente all'esecuzione del contratto. D'altra parte, ciò accade anche nell'ordinaria esecuzione di un contratto non concluso per il tramite di algoritmi, dove spesso, solo dopo la sua esecuzione, le parti si trovano a denunciare vizi dei beni ceduti. Appare, dunque, di fondamentale importanza trasporre nell'algoritmo tutte le circostanze e condizioni che devono essere considerate nell'esecuzione del contratto. Così come è di estrema importanza prestare attenzione a quelle regole che individuano i soggetti (c.d. *oracles*) deputati a fornire le informazioni e a definire la loro applicazione, escludendo qualsiasi forma di interpretazione. D'altronde, gli *smart contracts* si propongono di prevenire eventuali inadempimenti, eseguendo quanto in esso scritto senza necessità della collaborazione del fattore umano.

¹¹⁹ Si veda CUCCURU, *Blockchain ed Automazione Contrattuale. Riflessioni sugli smart contract*, cit., p. 107, in ordine alla dottrina che ha indagato l'uso di strumenti che incidono direttamente sul ventaglio di possibilità dei soggetti destinatari, deominati "*non-normative management*" (Brownsword, *In the Year 2061: from Law to Technological Management*, in *Law, Innovation and Technology*, Vol. 7, n. 1, 2015,

1), "*design-based regulation*" (Yeung, *Design for the Value of Regulation*, in *Van Den Hoven-Vermaas-Ven De Poel, Handbook of Ethics, Values, and Technological Design*, Springer, 2015) o, ancora, "*technological normativity*" (HILDEBRANDT, *Legal and Technological Normativity: more (and less) than twin sisters*, in *Techné*, Vol. 12, n. 3, 2008, 169).

4.1. *La natura giuridica dello smart contract.*

Lo smart contract non sempre corrisponde ad accordi giuridicamente vincolanti. Infatti, lo schema attuativo può ad esempio stabilire il pagamento in moneta digitale, entro una certa data, in esecuzione a un accordo già intervenuto fuori dall'ambiente virtuale o può prevedere un meccanismo per un processo non contrattuale, come nel caso di gestione di una procedura di voto non giuridicamente vincolante. In altri casi, invece, l'automazione può inerire anche la formazione del contratto stesso, mediante l'impiego di algoritmi che definiscono il contenuto contrattuale utilizzando applicazione dell'intelligenza artificiale¹²⁰. È chiaro che per l'individuazione della disciplina da applicare appare di primaria importanza ricostruire il fenomeno e indagare se la volontà delle parti si esprima per mezzo degli *smart contracts* o gli *smart contracts* non facciano altro che eseguire un accordo *off chain*. Si possono, dunque, riscontrare *smart contracts* che stabiliscono un processo computazionale; *smart contracts* che, invece, sono atti di esecuzione di un contratto; *smart contracts* che oltre a stabilire un processo computazionale siano anche un contratto nel senso giuridico del termine poiché creano, modificano, trasferiscono diritti, doveri e poteri. Quest'ultima fattispecie è probabilmente quella più interessante dal punto di vista giuridico, poiché si esce fuori dai canoni classici, in quanto è lo stesso codice informativo ad esprimere la dichiarazione intesa a realizzare un contenuto giuridicamente vincolante, da imputarsi direttamente al soggetto al quale il codice è legato, che attua secondo quanto programmato¹²¹.

Tuttavia, non tutto ciò che è giuridicamente rilevante è eseguibile. Ci sono, infatti, tutte una serie di clausole non implementabili, perché eccessivamente vaghe o interpretabili e, dunque, non matematicamente esprimibili in codici informatici. Si pensi, ad esempio, al principio di correttezza e buona fede, a quello della massima diligenza o alla clausola che si riferisce all'inadempimento grave o alla giusta causa¹²² quale criterio discrezionale per ritenere il recesso valido ed efficace.

¹²⁰ Si veda A. J. CASEY e A. NIBLETT, *Self-driving contracts*, visibile al sito <http://ssrn.com>, dove si ipotizza il caso in cui all'algoritmo è lasciato il compito di definire il contenuto del contratto.

¹²¹ Altri ritengono che invece gli *smart contract* siano più che altro uno strumento per la negoziazione e/o adempimento automatico di accordi digitalmente espressi. (Cucuru, *Blockchain ed Automazione Contrattuale. Riflessioni sugli smart contract*, cit., pag. 118).

¹²² Si tratta di clausole generali per le quali Mengoni ha autorevolmente sostenuto "Le clausole generali.. impartiscono al giudice una misura, una direttiva per la ricerca della norma di decisione: esse sono una tecnica di formazione giudiziale della regola da applicare al caso concreto, senza un modello di decisione precostituito da una fattispecie normativa astratta" L. MENGONI, *Spunti per una teoria delle clausole generali*, in *Riv. critica dir. priv.*, 1986, 10.

Oltre ai problemi di confezionamento del contratto *smart*, ulteriori questioni sorgono in ordine alla possibilità di intervenire su uno *smart contract* concluso e lanciato nella blockchain nel caso in cui debba essere eseguito un provvedimento inibitorio emesso dall'autorità giudiziaria. Al momento per realizzare un tale risultato, non si potrà che pensare ad una blockchain del tipo privata, con una *governance* che preveda meccanismi automatici di esecuzione o bloccaggio e l'individuazione di soggetti responsabili e deputati ad intervenire. Ciò sicuramente va contro la filosofia di base della tecnologia blockchain e crea una debolezza dal punto di vista della autonomia e sicurezza della ambiente in cui opera lo *smart contract*. Tuttavia, una tale soluzione consentirebbe, tra l'altro, la creazione di un punto di contatto tra sistema giuridico e sistema informativo, in quanto le decisioni giudiziali e le istanze tra le parti avrebbero dei destinatari concreti ¹²³.

Credo tuttavia che la questione non sia tanto l'individuazione del soggetto, facilmente regolabile con la identificazione al momento del rilascio dell'identità con la quale opera nella rete, quanto piuttosto di intervenire con un provvedimento esecutivo sul contratto stesso, per sua natura non modificabile. Il problema a mio parere non è (solo) giuridico, ma piuttosto tecnologico, in quanto dovranno prevedersi dei meccanismi tali che consentano di inibire l'esecuzione della prestazione nel caso in cui questa non abbia avuto inizio ovvero di consentire, ad esempio, il sequestro del bene ¹²⁴, anche nella sua forma liquida digitale nel caso in cui costituisca, ad esempio, provento di un reato o sia soggetto ad una esecuzione forzata specifica.

La struttura dello *smart contract* è caratterizzata da tre elementi: il codice di un programma che diventa l'espressione di una logica contrattuale (pagamento dell'indennizzo nell'ipotesi di verifica della condizione dedotta nel programma); i messaggi inviati dagli *oracles* alla blockchain, con la funzione di registrare gli eventi che devono far attivare le conseguenze stabilite (ad esempio il ritardo del volo); un meccanismo che preveda l'adempimento automatico (accredito del conto corrente del beneficiario della polizza).

¹²³ P. CUCCURU, *loc. ult. cit.*, p. 118 ss.

¹²⁴ Con riferimento alla sequestrabilità di criptovalute e, dunque, di codici informatici espressivi di un certo valore, il Tribunale di Brescia - Sez. specializzata in materia di Imprese con Decreto n. 7556/2018 (RG n. 2602) del 18 luglio 2018, nel rigettare il ricorso di una Società contro il rifiuto del notaio di provvedere all'iscrizione nel Registro delle Imprese di una delibera di aumento del capitale sociale con

conferimento di criptovaluta, ha tra l'altro rilevato l'impossibilità di eseguire un ipotetico pignoramento sulla criptovaluta, stante l'esistenza di dispositivi di sicurezza ad elevato contenuto tecnologico che impedirebbero, senza la collaborazione del debitore, l'espropriazione forzata. V. in Gazzetta notarile, <http://www.gazzettanotarile.com/gazzetta/index.php/sentenze/831-trib-brescia-decreto-18-luglio-2018-n-7556>, sito consultato il 30.10.2018.

Dal punto di vista operativo, perché lo *smart contract* funzioni è necessario o il consenso tra le parti e la presenza di un parte terza che ne garantisca l'affidabilità e ne impedisca manomissioni, come accade nella piattaforma di *eBay*, dove vi sono *smart contracts* che eseguono le clausole del contratto che gli utenti sottoscrivono quando si affidano a *eBay*¹²⁵, oppure necessitano il consenso delle parti e un meccanismo che, in modo automatico e senza possibilità che qualcuno possa bloccare l'esecuzione, si sostituisca all'intermediario ed esegua quanto trasposto dalle parti nel *software*. Questa modalità applicativa è ora possibile grazie alla blockchain.

L'ambito applicativo degli *smart contracts* è piuttosto ampio, si pensi, ad esempio al settore della musica o comunque in tutti i casi in cui occorre versare una *royalty* al titolare in ragione dell'utilizzo del bene o del servizio¹²⁶. Chiaramente, stante l'impossibilità dell'algoritmo di effettuare valutazioni in ordine all'esecuzione di una clausola, l'esecuzione automatica è evidentemente più congeniale a tutte le vicende contrattuali sottoposte a termine o a condizione, il cui accertamento potrà, ad esempio, avvenire tramite siti *web* istituzionali, come nel caso dei contratti di borsa, o attraverso i servizi degli *oracles*, come nel caso di verifica della qualità di un servizio o il riscontro di condizioni come lo stato avanzamento lavori di un appalto o le condizioni meteo in un luogo determinato¹²⁷.

È evidente che il funzionamento efficiente di un contratto intelligente richieda una fonte affidabile di dati che lo alimenti, attraverso gli *oracles*, sufficientemente protetta da attacchi *hacker*, che potrebbero minare l'affidabilità dello stesso contratto di eseguire nei termini concordati il codice informatico. Si pensi alla notizia non veritiera di ritardo di un volo tale per cui fa scattare la clausola di pagamento immediato e irreversibile in favore di

¹²⁵ Le clausole del contratto che i contraenti sottoscrivono quando si affidano a *eBay*; questi *smart contract* vengono eseguiti sui server della società di aste e vendite online.

¹²⁶ Fanno già utilizzo di questi contratti Artlery (<https://artlery.com>), che garantisce all'artista una percentuale per ogni passaggio di proprietà dell'opera avvenuto a mezzo di *smart contract* nella relativa blockchain, una sorta di diritto di seguito inestinguibile e senza frontiere e Maecenas (<https://www.maecenas.co>) piattaforma di *art-investment blockchain-based*, che raccoglie investimenti per favorire la proprietà diffusa, in *share*, di opere d'arte di gallerie e musei.

¹²⁷ Un esempio concreto di funzionamento di uno *smart contract* attivato dagli

input provenienti dall'esterno è il caso di una compagnia di assicurazioni che offre una polizza (*flightdelay*) che risarcisce i viaggiatori se il loro aereo subisce dei ritardi. La modalità di denuncia del sinistro è infatti del tutto automatica, poiché l'assicurato non deve comunicare alcunché, le informazioni sui voli verranno infatti acquisite automaticamente, e in tempo reale, da una società di informazione indicata nel contratto stesso. Il premio e il risarcimento sono pagati in Ether, la critpovaluta della blockchain Ethereum. Lo *smart contract* si attiverà automaticamente e darà seguito al risarcimento senza la necessità di un intervento umano non appena i dati dei voli comunicati alla blockchain non rileveranno un ritardo risarcibile ai sensi della polizza. Il sito della società è consultabile in <https://fdd.etherisc.com>.

tutti i beneficiari della polizza *smart* eseguita nella blockchain. Per tale ragione, stante la mancanza di affidabilità nei confronti di tali meccanismi, si è assistito ad uso limitato degli *smart contracts*. Una *start up*, *Chainlink*, ha recentemente sviluppato un sistema di *network* di oracoli decentralizzati (*ChainLink's oracle*)¹²⁸ resi tecnologicamente sicuri dall'utilizzo di crittografia in grado di rendere affidabile il flusso di informazione diretto verso la blockchain. La stessa società ha partecipato ad un progetto, *OpenLaw*¹²⁹ che dichiara di fornire *smart legal agreements* per “*create, store and excute legal agreements that interact with blockchain - based smart contracts without the need for any intermediaries*”.

Lo sviluppo dell'Intelligenza Artificiale¹³⁰ applicata agli *smart contracts* consentirà di aprire ulteriori nuovi fronti, che consentiranno di ridurre le possibilità di errori aumentando al contempo la conoscenza dei contenuti da parte dei sistemi.

4.2. *La forma dello smart contract.*

Negli *smart contracts* si pongono i medesimi problemi giuridici già analizzati nella disamina della blockchain in ordine all'identità delle parti e alla manifestazione delle dichiarazioni, poiché le parti di un contratto, agendo in forma di codici informatici e a distanza, debbono poter essere certi del soggetto al quale hanno indirizzato la propria dichiarazione e che tale dichiarazione giunga integra. Il tema dell'imputazione della dichiarazione contrattuale e della relativa integrità è connesso con la forma del contratto, mezzo attraverso il quale le parti manifestano il loro consenso.

Nel nostro ordinamento vige il principio della libertà della forma del contratto, ragione per la quale la manifestazione della volontà può avvenire con dichiarazione orale, comportamento concludente e dichiarazione per iscritto. Sotto l'aspetto “teleologico”, la forma della manifestazione del consenso, nel nostro ordinamento, può essere richiesta *ad substantiam* o *ad validitatem*, *ad probationem* e, secondo taluno, *ad regularitatem*¹³¹. Con riferimento alla particolare modalità di manifestazione del con-

¹²⁸ <https://medium.com/@OpenLawOf-ficial/openlaw-teams-with-chainlink-to-bring-real-world-info-to-smart-contracts-4e7a3dac80a8>.

¹²⁹ <https://www.openlaw.io>,

¹³⁰ L'Intelligenza Artificiale (o IA in italiano e *Artificial Intelligence* o AI in inglese) è un ramo dell'informatica che permette la programmazione e progettazione di sistemi sia hardware che software che permettono di dotare le macchine di determinate caratteristiche che vengono considerate tipicamente umane. In altre parole,

L'IA si occupa di realizzare macchine (*hardware* e *software*) in grado di “agire” autonomamente (risolvere problemi, compiere azioni, ecc.).

¹³¹ Sul punto si vedano: A. GENTILI, *La forma*, in *Lezioni sul contratto*, cit., p. 72; C.M. BIANCA, *Istituzioni*, cit., pp. 403-407. Con specifico riguardo alla forma telematica: D. NEGRONI, *I contratti conclusi via internet*, in www.ud.camcom.it, p. 5; A. VALONGO, *La conclusione del contratto mediante esecuzione nella contrattazione informatica*, in *Vita not.*, 2004, pp. 1286-1290;

senso negli *smart contracts* e, in genere, nei contratti telematici o cibernetici, pur nella loro differente struttura, il legislatore nazionale, dapprima con l. 15 marzo 1997, n. 59 e con il d.P.R. 10 novembre 1997, n. 513, poi trasfuso nel d.P.R. 28 Dicembre 2000, n. 445, e poi con il CAD, 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*”¹³². In tale caso, l’uso di un particolare tipo di firma dipenderà dalla forma scritta richiesta. Cosicché, l’art. 21, comma 2° *bis*, CAD stabilisce che nei casi in cui sarà necessario rispettare il requisito della forma *ad substantiam*¹³³ ex art. 1350 c.c., nn. 1-12, il documento informatico dovrà essere sottoscritto con firma elettronica qualificata o digitale, mentre gli atti di cui al n. 13 del medesimo articolo possono essere sottoscritti a pena di nullità non solo con firma elettronica qualificata o digitale, ma anche con firma elettronica avanzata. Qualora, poi, non si dovesse ricorrere all’utilizzo di una firma elettronica, l’imputabilità della dichiarazione espressa nel documento informatico ad un dato soggetto dovrà valutarsi tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità e il suo valore probatorio sono liberamente valutabili in giudizio¹³⁴.

4.3. *La manifestazione del consenso nell’automazione contrattuale e i criteri di imputazione della volontà.*

Nel richiamare quanto già illustrato in ordine alle firme elettroniche e alla loro valenza certificatoria, basti qui rilevare che al di là della evidente differenza dal punto di vista ontologico rispetto al contratto cartaceo, sebbene identico quanto ad effetti a quello informatico, ciò che invece viene in rilievo è il differente *tool* normativo che dovremo applicare allorquando ci troveremo di fronte ad uno *smart contract*. Non solo dunque le norme “generali” dettate dal codice civile in tema di contratto, ma anche quelle speciali oggi racchiuse nel regolamento eIDAS e CAD.

È stato scritto in ordine alla contrattazione telematica che si sta assistendo ad una progressiva oggettivazione del contratto, ormai divenuto “atomo di scambi telematici”, atto governato da una procedura standardizzata irreversibile, spersonalizzato e decon-

A. GENTILI, *Documento informatico e tutela dell’affidamento*, in *Riv. dir. civ.*, 1998, p. 163 ss.

¹³² L. 59/1997, art. 15 co. 2.

¹³³ Per le scritture private di cui all’art. 1350, comma 1, nn. da 1 a 12, c.c.

¹³⁴ Art. 20, CAD.

testualizzato rispetto al tempo e allo spazio¹³⁵. Parte della dottrina ha individuato nel contratto telematico, normalmente unilateralmente predisposto, una manifestazione di c.d. scambio senza accordo¹³⁶, in cui “l’autonomia non risulta più garantita dall’esercizio di forze psicologiche o dalla spontanea composizione di interessi”, potendosi oramai discorrere di autonomia privata, ma non anche di autonomia negoziale, e ciò in quanto “la teoria del negozio giuridico presuppone la singola e concreta parte; mentre l’economia contemporanea conosce soltanto anonimi e astratti consumatori”. Il contratto, dunque, sorgerebbe e si svolgerebbe in assenza di manifestazioni di volontà dei contraenti e l’applicabilità della disciplina del contratto dovrebbe essere il frutto di un’opzione dell’ordinamento che sceglie di trattare questa vicenda alla stregua di quella contrattuale. Altra dottrina preferisce parlare di rapporti contrattuali di fatto¹³⁷ e altra ancora¹³⁸, in adesione all’orientamento consensualistico, rileva la riaffermazione del principio negoziale in tutti i casi in cui vi sia libertà o meno di accettare l’accordo, ritenendo per contro insussistente l’accordo negoziale non tanto in difetto di trattative, ma esclusivamente in difetto del potere dell’oblato di rifiutare. Vi è, inoltre, chi ha ritenuto forzato ricondurre l’accordo ad un incontro di volontà, poiché in esso l’accordo sembra svanire per essere sostituito dall’incontro tra il “dialogo uomo macchina” e il “dialogo tra macchine”¹³⁹. Il codice civile (art. 1321) definisce il contratto l’accordo di due o più parti per costituire, regolare o estinguere tra loro un rapporto giuridico patrimoniale. Mancando l’accordo viene meno il contratto. Tuttavia, perché vi sia accordo non è necessaria la presenza di “trattative + dialogo”, bastando anche la presenza di due comportamenti da cui indurre il signi-

¹³⁵ Così C. CAMARDI, *Contratto e rapporto nelle reti telematiche. Un nuovo modello di scambio*, in *Trattato dir. comm. dir. pubbl. ec.* diretto da F. Galgano, cit., p. 14.

¹³⁶ N. IRTI, “Scambi senza accordo”, in *Rivista trimestrale di diritto e procedura civile*, Milano, 1998, *passim* (ed in particolare p. 176 ss.). Tale tesi origina dagli acquisti di beni nei grandi magazzini. Altra dottrina aveva già ritenuto che con riguardo ai contratti telematici potesse ritenersi mancante l’accordo negli elementi strutturali dei negozi di scambio, fino a giungere ad escludere tali negozi dalla categoria giuridica del contratto. Cfr. E. GIANNANTONIO, *Introduzione all’informatica giuridica*, Milano, 1984, p. 245.

¹³⁷ C.M. BIANCA, *Acontrattualità dei contratti di massa?*, in *Vita not.*, 2001, pp. 1123-1128.

¹³⁸ G. OPPO, *Disumanizzazione del contratto?*, in *Riv. dir. civ.*, 1999, p. 531; A. M. GAMBINO, *L’accordo telematico*, *passim*; F. GAZZONI, *Contatto reale e contatto fisico (oververosia l’accordo contrattuale sui trampoli)*, in *Riv. dir. comm.*, 2002, pp. 665-666.

¹³⁹ Così A. NERVI, *L’impiego del computer nel procedimento di formazione del contratto*, in *Trattato Galgano*, 2002, Milano, p. 131, con riguardo ai contratti cibernetici, nei quali si assiste alla sostituzione dell’operatore umano con un programma, inserito dallo stesso dichiarante o da un terzo programmatore, in grado di dotare la macchina di un’intelligenza artificiale (cfr. D. PARISI, *Intelligenza artificiale*, in *Enc. Scienze sociali*, Milano, 1996, p. 9 ss.; A. GENTILI, *Inefficacia e vizi della volontà nella contrattazione telematica*, in *Tratt. dir. comm. dir. pubbl. econ.*, diretto da F. Galgano, Padova, 2001, p. 144.

ficato negoziale secondo criteri di tipicità sociale¹⁴⁰. La categoria del contratto, come disegnata nel nostro codice, da un punto di vista strutturale “sfuma in una serie di congegni tecnici assai diversi”¹⁴¹, modellati a seconda dell’interesse delle parti, per cui appare una forzatura ricondurre le varie tipologie procedimentali entro uno schema unitario “proposta-accettazione”, (art. 1326). Si pensi, ad esempio al modello di cui all’art. 1327 c.c., in cui si prevede la conclusione del contratto per effetto dell’inizio dell’esecuzione della prestazione o al modello di cui all’art. ex 1333 c.c., in cui la proposta di concludere un contratto con obbligazioni a carico del solo proponente si perfeziona per il solo fatto del mancato rifiuto nel termine d’uso, senza bisogno d’alcuna accettazione¹⁴². La sintetica rassegna di alcune delle questioni giuridiche poste in ordine al contratto telematico si acquiscono se le poniamo per l’analisi dello *smart contract*, dove le tecnologie informatiche e telematiche non sono usate (solo) per veicolare una volontà già formata, ma anche per costituire esse stesse la volontà del soggetto, racchiusa in un algoritmo, scritto (con l’ausilio di tecnici) e voluto dallo stesso soggetto, che auto esegue le istruzioni impartitegli.

Tale ulteriore elemento¹⁴³, tuttavia, non sembra portare ad un nuovo modello di contratto, ma, tutt’al più, ad una diversa modalità di manifestazione del consenso, così come enucleata dal codice civile. È evidente che lo sviluppo tecnologico ci sta proponendo nuove forme di formazione e conclusione del contratto, che richiedono senz’altro, regole specifiche, come quelle sulla certificazione dell’identità di un soggetto, racchiuse nel regolamento eIDAS e nel CAD. Il trasferimento di diritti tramite registro distribuito per mezzo di contratti che auto eseguono le pattuizioni in esso stabile, senza l’intervento del fattore umano, apre un nuovo modo per l’autonomia privata di manifestare la propria libertà negoziale. Nell’ipotesi limite in cui è lo stesso codice informatico ad adottare l’esecuzione di una prestazione in ragione degli accordi raggiunti o di proporre esso stesso offerte, magari entro schemi predefiniti, al verificarsi di determinate condizioni, non sembra potersi escludere la presenza della preventiva mani-

¹⁴⁰ A. DI MAJO, *L’accordo*, in AA.VV., *Lezioni sul contratto raccolte da Andrea Orestano*, Cap. I, Torino, 2009, p. 1.

¹⁴¹ In tali termini G. BENEDETTI, *Dal contratto al negozio unilaterale*, Milano, 1969 (rist.), p. 1.

¹⁴² *Cassazione civile*, Sez. II, sentenza n. 26325 del 31 ottobre 2008.

¹⁴³ Gli *smart contracts*, e in special

modo quelli eseguiti nella blockchain, possono, in effetti, considerarsi un’evoluzione dei contratti telematici, caratterizzati fondamentalmente, oltre che dall’automazione nell’esecuzione del contratto, dalla modalità di formazione della volontà e dall’assenza del fattore umano per la loro attivazione.

festazione di volontà, sussistendo essa sin dal momento della programmazione¹⁴⁴.

Si potrebbe, dunque, assumere che in forza dei principi di auto responsabilità ed affidamento, colui che operi per il tramite di uno *smart contract* vi resterà vincolato, quant'anche gli vengano imputati effetti non voluti o dovuti a distorsioni o imprevedibilità della programmazione, salvo esercitare le opportune azioni di impugnativa o volte ad accertare un eventuale inadempimento del programmatore.

D'altronde, la dottrina ci ricorda che “vi possono essere casi nei quali il debitore non è inadempiente, ancorché non sia sopravvenuto il fortuito; e vi possono essere casi in cui la sopravvenienza del fortuito non implica di per sé, necessariamente e automaticamente, l'esonero del debitore”¹⁴⁵. Peraltro, lo *smart contract*, per come è congegnato, impatterà anche sull'impossibilità di non adempiere ovvero sull'attivazione di rimedi di autotutela o di istituti come la revoca del consenso. Sarà solo l'evoluzione tecnologica a consentire che un terzo (dotato evidentemente di specifici privilegi) possa intervenire — informaticamente — per bloccare l'esecuzione, perché, ad esempio, una nuova norma abbia reso l'oggetto del contratto illecito o in forza di un provvedimento giudiziario.

Dunque, se da un lato la trasposizione di clausole contrattuali in codici informatici consente di prevenire i problemi legati all'inadempimento, dall'altro lato tale modalità di manifestazione del consenso responsabilizza la parte ad un uso consapevole dello strumento informatico, al quale si è relegata la fase di formazione e/o esecuzione del contratto. Quindi, eventuali contestazioni, in linea generale, potranno essere vagliate solo in momento successivo.

Dalla analisi delle questioni sopra poste, non credo, quindi, che gli *smart contracts*, al momento, richiedano l'individuazione di fattispecie giuridiche nuove rispetto a quelle esistenti, pur incidendo, tale nuova forma contrattuale, sulle modalità di manifestazione del consenso. Si condivide, dunque, con quella dottrina che con riguardo ai contratti cibernetici ritiene che “siamo di fronte a fenomeni in cui la volontà opera su piani diversi nell'ambito del procedimento di formazione del contratto: a) v'è nel momento iniziale, in cui il contraente decide di ricorrere allo

¹⁴⁴ Si pensi ai *software agents* che agiscono, sotto il profilo tecnico-informatico e socio-relazionale, come fossero dei “rappresentanti” (agent) dell'utente, stabilendo con un certo grado di autonomia se stipulare o meno il contratto, a quali condizioni e con quali contenuti. Per un'ampia analisi del fenomeno v. F. BRAVO, *Contratto ciber-*

netico, in *Dir. informatica*, fasc. 2, 2011, pag. 169.

¹⁴⁵ G. ALPA, *Il contratto in generale*, Fonti, teorie, metodi, nel *Trattato Cicu-Messineo-Mengoni*, continuato da Schlesinger, XIV, 1, Milano, 2014, p. 283.

strumento tecnologico (cibernetico) per lo svolgimento dell'attività contrattuale; b) si ha anche nel momento in cui il soggetto intende avvalersi dello strumento tecnologico per integrare la propria volontà nella formazione del regolamento di interessi definitivo; c) la volontà emerge infine 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 giuridici”¹⁴⁶.

Si ritiene, quindi, che la decisione di avvalersi di un *software*, programmato per eseguire delle istruzioni informatiche, siano elementi sufficienti per imputare tutte le dichiarazioni negoziali elaborate, eseguite e trasmesse al soggetto che ha assunto tali decisioni. Pur volendo prendere atto dell'autonoma capacità elaborativa dell'assetto tecnologico adottato (codice informatico che esegue le istruzioni impartite e la blockchain che valida ed esegue), non sembra che si possa giungere ad una soggettivazione del codice informatico, il quale rappresenterebbe esclusivamente lo strumento di manifestazione di una volontà e di esecuzione di un accordo in altro modo raggiunto¹⁴⁷. Allo stesso modo, sul piano della distribuzione del rischio, la responsabilità e l'inadempimento saranno imputati alla parte che si avvale dell'algoritmo, conformemente ai “confini negoziali o quelli propri del tipo contrattuale prescelto”¹⁴⁸. In una prospettiva *de iure condendo*, è in discussione in sede europea l'opportunità di introdurre una nuova categoria giuridica, quella delle “persone elettroniche” veri robot autonomi e decisionali, responsabili di qualsiasi danno da essi causato, “dal momento che le macchine progettate per scegliere le loro controparti, negoziare termini contrattuali, concludere contratti e decidere se o cioè attuarli rendono inapplicabili le norme tradizionali”¹⁴⁹.

¹⁴⁶ F. BRAVO, *Contratto cibernetico*, in *Dir. informatica*, fasc.2, 2011, pag. 169 ss.

¹⁴⁷ Non mi sembra, in definitiva, che si possa mettere in dubbio la presenza dell'elemento della volontà negli *smart contracts*, né, quindi, la conseguente e piena applicabilità delle norme concernenti i vizi del consenso (artt. 1427-1441 c.c.). Si veda R. Borruso, cit., p. 350, il quale con riguardo ai contratti cibernetici, parla di “volontà voluta se non volente”, in cui peraltro la parte, avvalendosi del computer per manifestare la propria volontà, accetterebbe preventivamente il rischio informatico, nell'esercizio di un'autonomia contrattuale che l'ordinamento gli riconosce e che quindi non può essere causa di invalidità del contratto.

Un maggior sforzo intellettuale sicuramente dovrà essere fatto, prima ancora che

per la ricerca del tipo, per comprendere il contesto informatico in cui prende forma l'autonomia privata, non solo da parte degli interpreti del diritto, ma anche da parte dei soggetti del rapporto, affinché accrescano quella consapevolezza necessaria per gestire gli effetti del prodotto dalle nuove tecnologie. Sulle difficoltà connesse al mancato possesso delle competenze informatiche necessarie da parte degli operatori del diritto in generale e dei giudici in particolare, cfr. CUCURU, *Blockchain ed automazione contrattuale*, cit., p. 107 ss.

¹⁴⁸ G. ALPA, *Il contratto in generale*, *Fonti, teorie, metodi*, cit., p. 285.

¹⁴⁹ Si veda la “Risoluzione del Parlamento europeo del 16 febbraio 2017 recante Raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica”, in <http://www.europarl.europa.eu/sides/>

5. CONCLUSIONE.

Nel 2001 Natalino Irti¹⁵⁰ affermava che la globalizzazione nella rete telematica raggiunge il suo grado più elevato e rilevava, altresì, che nello spazio telematico non sono certo individuabili i luoghi dei singoli computer; si tratta in effetti di un non - luogo, poiché i luoghi appartengono a terra, mare e aria. La globalizzazione ha modificato profondamente il sistema delle fonti di produzione del diritto, giacché il diritto essendo destinato a trovare applicazione oltre ogni confine statale tende a formarsi nei diversi punti del pianeta¹⁵¹.

È già accaduto con Internet, la rete delle reti¹⁵², per sua natura estesa in tutto il pianeta, decentrata e priva di gerarchia, che non consente il ricorso ai tradizionali strumenti utilizzati per ancorare una determinata fattispecie ad un luogo e, quindi, ad una norma applicabile¹⁵³. Con la blockchain tutto si acuisce, poiché è assente del tutto il fattore umano, il soggetto intermediario che in Internet garantisce lo sviluppo del mercato virtuale.

Occorre ripensare il rapporto tra codice informatico e legge considerata la forte collisione tra la blockchain e le leggi attuali, pensate per un paradigma socio-economico in cui vi è sempre un soggetto gestore, controllore e, dunque, responsabile, al quale gli atti sono imputabili. Si pensi alle organizzazioni lanciate nella blockchain, le c.d. DAO (*Decentralized Autonomous Organization* o organizzazioni autonome decentralizzate) operanti attraverso *smart contracts*, che funzionano interamente senza l'intervento umano e grazie ad un codice autonomo, dove il consenso del soggetto nei cui confronti si realizzano gli effetti delle attività del *software* verrebbe espresso (solo) nella fase iniziale di adesione.

L'assenza di confini territoriali e di frontiere fisiche, nello spazio virtuale, comporta la necessità di riconsiderare nella regolamentazione giuridica delle relazioni che si dipanano nella rete. Il diritto deve, quindi, porsi alla ricerca di forme di regolazione disancorate dal territorio. Nasce un duplice ordine di problema, poiché si tratta di comprendere e decidere, da un lato, la fonte normativa che si fa carico di disciplinare le nuove relazioni economiche "virtuali" e, cioè, se debba essere di livello sovranazionale¹⁵⁴, dall'altro lato, come logico corollario, si tratta

getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//IT.

¹⁵⁰ N. IRTI, *Norme e luoghi. Problemi di geo-diritto*, cit., p. 65.

¹⁵¹ In questo senso F. GALANO, *La globalizzazione nello specchio del diritto*, Bologna, 2005, p. 34 ss.

¹⁵² Tale attributo nasce dal confronto di Internet come rete estesa in tutto il globo

con le reti telematiche che coprono un'area minore, come quelli locali (c.d. reti L.A.N. = *Local Area Network*).

¹⁵³ C. ROSSELLA, *Commercio elettronico. La governance di Internet tra diritto statale, autodisciplina, soft law e lex mercatoria*, Milano, 2006 cit., p. 5.

¹⁵⁴ G. ALPA, *New economy e nuove professioni: il diritto privato e l'attività fo-*

di ricercare forme di regolazione disancorate dal territorio, che consentano la *governance* dell'economia elettronica transnazionale¹⁵⁵. La dottrina più attenta allo studio delle dinamiche giuridiche nel mondo virtuale, nel tentativo di rispondere alla domanda su quale fosse la forma di *governance* possibile e più confacente per il commercio elettronico ha schematizzato le soluzioni riconducendole a tre modelli di fondo: a) il primo vedrebbe Internet regolato dal diritto attualmente vigente statuale o convenzionale; b) il secondo ritiene necessarie innovazioni tanto del diritto quanto delle fonti per adeguarli ai fenomeni giuridici che si spiegano nel cyberspazio; c) il terzo ritiene che Internet non debba essere governato da nessuna normativa ovvero esige un ordinamento speciale governato da una *lex informatica*¹⁵⁶. Altra dottrina¹⁵⁷ parla, invece, di "*lex cryptographica*", quale ordinamento privato entro il quale operano i *framework* basati su un codice informatico e lanciati nella blockchain. La blockchain ha bisogno, tuttavia, della stabilità e della prevedibilità che lo stesso Reidenberg invoca. Un governo della rete lasciato alla *lex informatica* o *cryptographica* porterebbe alla formazione di regole tecniche al di fuori del processo democratico, creando, al contempo un ordinamento parallelo al mondo reale.

La domanda è, quindi, se la blockchain può essere effettivamente autoregolata in modo autonomo rispetto agli ordinamenti giuridici di un dato paese, nel cui ambito deve esplicare effetti. È plausibile ritenere che affinché le attività negoziate nella blockchain esplichino effetti anche nel mondo reale, quelle stesse attività debbano essere sussunte in una norma giuridica che conferisca loro effetti giuridici¹⁵⁸. Difatti se i risultati di una transazione intercorsa tra due soggetti nella blockchain non ha protezione nel mondo reale, il valore di tale nuovo paradigma economico è significativamente depotenziato. La certezza delle relazioni è legata alla effettiva possibilità delle parti di far valere

rense nell'era della rivoluzione digitale, in *Contratto e impresa*, 2000, p. 1175.

¹⁵⁵ C. ROSSELLA, *op. ult. cit.*, p. 8.

¹⁵⁶ R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, in *Texas Law Review*, cit., p. 553 ss. Tale orientamento nasce dalla constatazione del condizionamento che la tecnologia esercita non soltanto nelle modalità di trasmissione delle informazioni, ma anche su scelte che condizionano la disciplina del rapporto. Si tratta di regole interne alla rete, sviluppate attraverso soluzioni tecnologiche, disancorate dalle norme statuali e, quindi, di facile attuazione mediante il controllo dello strumento tecnico.

¹⁵⁷ Si veda P. DE FILIPPI e A. WRIGHT, *Blockchain and Law, The Rule of Code*, Harvard University Press, 2018, *passim*.

¹⁵⁸ In ordine al procedimento di sussunzione del fatto alla norma si è osservato che « di fronte ad ogni fatto sociale l'ordinamento giuridico deve prendere posizione. In quanto prende posizione ... esso non fa altro che dichiarare la esigenza che si produca ... un determinato effetto. Questo evento avrà sempre ... una fisionomia definita: la quale potrà essere espressa concettualmente in un *nomen iuris* ». V. A. FALZEA, *Ricerche di teoria generale del diritto e di dogmatica, Teoria generale del diritto*, Milano, 1999, 17.

un proprio diritto. Il legislatore determina i mezzi, le regole e gli effetti per l'applicazione dei diritti e l'estensione delle tutele.

La tecnologia dei registri distribuiti per poter essere sviluppata nel pieno delle sue potenzialità deve trovare un posto all'interno di un quadro normativo adeguatamente strutturato, pertinente e versatile, in grado di svilupparsi *pari passu* con lo sviluppo tecnologico in atto. Il codice informatico deve, dunque, considerare la norma, non può essere avulsa da essa, e deve impegnarsi in una interazione che tenda ad eliminare i conflitti.

La norma, chiaramente, non può essere (solo) quella di un determinato Stato. Sulla scia di quanto sta accedendo a livello europeo in ordine ai mezzi di identificazione elettronica e servizi fiduciari ¹⁵⁹ e all'adozione di soluzioni basate sulla blockchain, appare necessario adottare un approccio che tenda ad "adeguare" il sistema delle fonti normative e che preveda una "interoperabilità" di strumenti di regolazione autoritativa e di disciplina convenzionale a livello internazionale, al fine di scongiurare una produzione normativa locale, inadatta a regolare fenomeni sociali globali, come quelli in atto, disancorati da un territorio specifico e, dunque, difficilmente regolabile con il diritto di un (solo) ordinamento giuridico. Alcune forme di blockchain, specie quelle private, potranno inserirsi già nell'attuale quadro normativo esistente, altre avranno bisogno di nuove regole al fine di dare certezza giuridica ai soggetti e al mercato e linfa vitale allo sviluppo di ecosistemi emergenti. In tale quadro, la *lex informatica*, intesa come un insieme di regole tecniche ¹⁶⁰ (rappresentate dalle strutture tecnologiche e dagli *standard* di rete) ¹⁶¹ che veicolano scelte giuridiche e che impongono dei comportamenti agli utenti della Rete, costituirebbe una fonte oggettiva di integrazione del contratto ex art. 1374 c.c. Il contratto, quindi, diventerebbe lo "strumento della innovazione giuridica", e "non già le leggi", non necessarie per regolare la nuova economia ¹⁶². L'accordo delle parti unitamente all'apporto di altri elementi ad

¹⁵⁹ Il regolamento eIDAS prevede che ciascuno stato membro possa notificare i sistemi di identificazione elettronica forniti ai cittadini, al fine di adeguare il mercato unico dell'UE all'era digitale, abbattendo le barriere normative e passando dagli attuali 28 mercati nazionali a un mercato unico digitale di identità digitale. Successivamente, con la Decisione di esecuzione (UE) 2015/296 del 24 febbraio 2015, la Commissione, conformemente all'articolo 12, paragrafo 7, del regolamento, fissa le modalità procedurali necessarie per facilitare la cooperazione fra gli Stati membri nella misura in cui ciò sia necessario per garantire l'interoperabilità e la sicurezza dei regimi di

identificazione elettronica che gli Stati membri hanno notificato, o intendono notificare, alla Commissione.

¹⁶⁰ Si tratta di protocolli informatici, del software, dell'hardware, degli algoritmi e del codice binario con cui i programmatori informatici strutturano ed architettano la Rete, stabilendo i vari modi d'uso delle tecnologie informatiche.

¹⁶¹ È la schematizzazione suggerita da J.R. REIDENBERG, *op. ult. cit.*, 566.

¹⁶² Si veda in tal senso F. GALGANO, *Diritto ed economia alle soglie del nuovo millennio*, in *Contratto e impresa*, 1, 2000, 197.

esso esterni andrebbe dunque a comporre il regolamento contrattuale, che diventerebbe il risultato tra “voluto + normato”¹⁶³. Purtuttavia, proprio nella prospettiva di tale integrazione, appare imprescindibile un approccio al fenomeno globale e coordinato¹⁶⁴, secondo una prospettiva che guardi gli interessi da tutelare alla luce delle nuove tipologie dei servizi e delle opportunità che le nuove tecnologie mettono a disposizione¹⁶⁵. Fondamentale sarà il confronto tra sviluppatori, regolatori e legislatori in un contesto necessariamente internazionale, al fine di creare un *framework* sovranazionale, pensato come *standard* internazionale, incline all’evoluzione tecnologica, ma allo stesso tempo attento alla tutela dei diritti dell’individuo e delle imprese.

¹⁶³ Così G. ALPA, *Corso di diritto contrattuale*, Milano, 2006, p. 5, il quale rileva che “dal contratto quale manifestazione o dichiarazione di volontà, c.d. voluto, si distingue il *regolamento contrattuale*, composto da *voluto+normato*”.

¹⁶⁴ L’antagonismo tra giurisdizioni nel fornire una regolamentazione specifica alla

blockchain favorirà senz’altro lo sviluppo della blockchain.

¹⁶⁵ Si vedano in questo stesso senso le conclusioni cui giunge Rossello in ordine alla regolazione del commercio elettronico in C. ROSSELLO, *Commercio elettronico*, cit., p. 21.