Il diritto digitale
Temi di informatica giuridica

a cura di
Monica Palmirani, Giovanni Sartor
Federico Galli, Salvatore Sapienza

Bologna
University Press

IL DIRITTO DIGITALE
Temi di informatica giuridica

a cura di
Monica Palmirani, Giovanni Sartor
Federico Galli, Salvatore Sapienza

Bologna
University Press

Title: LEGAL DESIGN AND DATA SCIENCE FOR EXPLICABLE AI IN LEGAL DOMAIN
Acronym: LEDS 4 XAIL
n. GPA: 101085576
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Education and Culture Executive Agency (EACEA). Neither the European Union nor the granting authority can be held responsible for them.

Fondazione Bologna University Press
Via Saragozza 10, 40123 Bologna
tel. (+39) 051 232 882

www.buponline.com
e-mail: info@buponline.com

ISBN 979-12-5477-771-8
ISBN on line 979-12-5477-772-5
DOI 10.30682/9791254777725

Questo volume è stato realizzato a partire da un impaginato camera-ready in formato pdf fornito dai curatori

In copertina: Summit Art Creations/Shutterstook.com

Prima edizione: marzo 2026

INDICE

SMART CONTRACT E BLOCKCHAIN

Chantal Bomprezzi

SOMMARIO: 1. Inquadramento tecnologico. 2. *Smart Contract* e *Smart Legal Contract*. 3. *Smart Contract* e *Data Act*. 4. *Blockchain* e Regolamento Eidas. 5. *Blockchain* e protezione dei dati personali. 6. Smart contract, Nft e metaverso. 7. *Blockchain* e *self-sovereign identity*.

1. Inquadramento tecnologico

Gli *smart contracts* sono programmi informatici deterministici che si auto-eseguono sulla *blockchain* in base alle istruzioni ricevute, inscritte nell'algoritmo che li governa. Possono definirsi deterministici in quanto, a fronte di uno specifico *input,* restituiscono un *output* predeterminato, essendo la loro esecuzione prevedibile *ex ante*. Con auto-esecuzione si intende, invece, l'attuazione, ad opera del programma, di azioni prestabilite al ricorrere di condizioni codificate, secondo la logica "se X, allora Y"[1]. Gli *smart contracts*, pertanto, contrariamente a quanto l'accezione potrebbe evocare, non sono necessariamente contratti. Questa obiezione, invero, non è dovuta alla natura (informatica) del linguaggio utilizzato. Lo *smart contract*, infatti, ben potrebbe rappresentare il mezzo mediante cui si articola la volontà delle parti, espressa sotto forma di linee di codice[2], sia a mente del principio di libertà delle forme, che del principio internazionale di non discriminazione[3] (per cui a qualsiasi documento non può essere negata validità per il solo fatto di essere in forma elettronica). Piuttosto, si evidenzia che presupposto imprescindibile per l'esistenza di un contratto sia l'accordo tra le

---

[1] P. CUCCURU, *Blockchain ed automazione contrattuale, riflessioni sugli smart contract*, in *Nuova giur. civ.*, 2017 (I), pp. 107-119; ID., *Beyond Bitcoin: an early overview on smart contracts*, in *International Journal of Law and Information Technology*, 2017 (XXV), pp. 179-195.

[2] M. DUROVIC, A. JANSSEN, *The Formation of Blockchain-based Smart Contracts in the Light of Contract Law*, in *European Review of Private Law*, 2019 (VI), p. 760.

[3] Il principio di non discriminazione è stato introdotto nel 1996 dalla Commissione ONU sul commercio internazionale (UNCITRAL) con il *Model Law on Electronic Commerce* (MLEC), all'art. 5, poi incluso nel 2005 nella *United Nations Convention on the Use of Electronic Communications in International Contracts,* all'art. 8. Sui due testi, vedi L. CASTELLANI, *I testi dell'UNCITRAL in materia di diritto del commercio elettronico*, in G. FINOCCHIARO, F. DELFINI (a cura di), *Diritto dell'informatica*, Milano: Utet, 2014, pp. 44-46.

parti; pertanto, in assenza di esso, lo *smart contract* non può considerarsi alla stregua di un contratto, nonostante contenga in sé la rappresentazione di clausole contrattuali. Diversamente, chiunque potrebbe caricare unilateralmente uno *smart contract*; la mera registrazione in *blockchain* non sarebbe elemento sufficiente a ipotizzare la presenza di una volontà comune[4].

Seppur gli *smart contract* non siano di per sé contratti, né debbano avere necessariamente una rilevanza legale, certamente possono essere utilizzati in ambito contrattuale per la conclusione e/o esecuzione di contratti[5]. Se utilizzati in ambito contrattuale, vengono usualmente denominati "*smart legal contracts*", per rimarcare la differenza con lo "*smart contract code*"[6]. In aggiunta, essi possono operare indipendentemente dalla *blockchain*, essendo addirittura antecedenti alla sua invenzione[7].

Nel panorama *blockchain*, gli *smart contracts* rientrano tra le applicazioni più evolute. La collocazione di uno *smart contract* in *blockchain* consente di trarre vantaggio dalle caratteristiche di quest'ultima, in particolare la capacità di resistenza alle manomissioni (o immutabilità) e la decentralizzazione[8].

La *blockchain* è un sistema distribuito, i cui dati sono replicati in copie dislocate in molteplici dispositivi elettronici, o "nodi", essendo conseguentemente la loro perdita meno probabile. Inoltre, i dati inseriti in *blockchain* sono abbinati a degli "*hash*", delle stringhe alfanumeriche univoche che variano al mutare del dato sottostante, raggruppati in blocchi. Ogni blocco ha il proprio *hash* identificativo che riporta al suo interno anche l'*hash* del blocco cronologicamente antecedente, fino a formare una catena (da cui il termine "*blockchain*", o "catena di blocchi"). Grazie a questa particolare conformazione, ogni tentativo di cambiamento può essere immediatamente individuato, giacché determinerebbe la modifica dell'*hash* e di quelli successivi, che sarebbero a loro volta difformi dagli *hash* corrispondenti posti negli altri nodi della *blockchain*. La decentralizzazione,

---

[4] C. SILLABER, B. WALTL, *Life Cycle of Smart Contracts in Blockchain Ecosystems,* in *Datenschutz und Datensicherheit*, 2017 (VIII), pp.498-499. I due autori osservano che: «*although a smart contract has been stored on the blockchain, this fact alone should not be considered as a party's agreement to enter the contract as anybody can submit any smart contract to the blockchain indicating an obligation for any random wallet owner*».

[5] La piattaforma più famosa è Ethereum (https://ethereum.org/it/).

[6] J. STARK, *Making Sense of Blockchain Smart Contracts, CoinDesk*, 7 giugno 2016, https://www.coindesk.com/making-sense-smart-contracts.

[7] Vedi *infra*, par. 2.

[8] Lo EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM, *Legal and Regulatory Framework of Blockchains and Smart Contracts*. 27 settembre 2019, https://www.eu blockchainforum.eu/reports, dà la seguente definizione di *smart contract*: «*In the blockchain context, it generally means computer code that is stored on a blockchain and one or more parties can access that. These programs are often self-executing and make use of blockchain properties like tamper-resistance, decentralised processing, and the like*» (p. 22).

invece, concerne il peculiare meccanismo di duplicazione del dato in molteplici copie; mentre esso avviene normalmente a partire da un nodo centrale, in *blockchain* l'aggiornamento del database viene effettuato in contemporanea su tutti i nodi grazie alle regole stabilite da un protocollo informatico comune, o meccanismo di consenso[9]. Tale modalità consente di evitare i costi e gli eventuali errori di trasmissione del dato da un nodo all'altro, a vantaggio della trasparenza delle informazioni da condividere e di una maggiore efficienza, sia in termini di tempo che economici[10].

Esistono svariate tipologie di blockchain. Si suole distinguere normalmente tra *blockchain permissionless* e *permissioned*. La differenza sta nei permessi conferiti ai soggetti che prendono parte alla *blockchain* mettendo a disposizione un proprio nodo. Nello specifico, vi sono anzitutto il permesso di scrivere (cioè di generare nuove transazioni) e di aggiornare la *blockchain* aggiungendo nuovi blocchi. Nelle *blockchain permissionless*, chiunque può divenire un utente e inserire dati in *blockchain*, oltre che aggiornare il *database* mediante la validazione delle transazioni effettuate. Nelle *blockchain permissioned*, tali permessi sono concessi solamente a taluni soggetti preidentificati. Un ulteriore permesso concerne la lettura di quanto incluso in *blockchain*. Le *blockchain permissionless* sono solitamente ad accesso pubblico, mentre le *blockchain permissioned* sono generalmente private, poiché le transazioni sono visibili solo agli utenti autorizzati. La ragione sta nel

---

[9] Il protocollo di consenso più noto prende il nome di "*Proof of Work*" (PoW), e consiste in una competizione tra nodi (*miners*); il primo tra questi che risulti capace di risolvere un complesso problema matematico, trovando un *hash* che sia composto da un numero predeterminato di zeri nella parte iniziale, è legittimato ad inserire un nuovo blocco e a ricevere una ricompensa per il lavoro svolto. Tuttavia, ci sono centinaia di diversi meccanismi di validazione che si basano su diverse strategie del consenso. Un'altra modalità molto citata è la "*Proof of stake"* (PoS) che si basa sulla validazione delle informazioni da parte di coloro che hanno più risorse (e.g., bitcoin, potenza di calcolo, etc.). Tali meccanismi sono stati suddivisi in tre famiglie: consenso basato su algoritmi che dimostrano l'esistenza di un certo criterio sulla base di un lavoro-work (es. PoW; PoS; *Proof of Reputation* (PoR); etc.); algoritmi basati sulla votazione di nodi qualificati (es. *Delegated Proof of Stake* (DPoS); *Random Lottery*, etc.); algoritmi basati sull'autenticazione dei nodi nei quali si registrerà la transazione (es. *Proof-of-Authentication* (PoAh)). Sul tema, vedi A. SINGH *et al.*, *A survey and taxonomy of consensus protocols for blockchains*, in *Journal of Systems Architecture*, 2022 (CXXVII), https://www.sciencedi rect.com/science/article/abs/pii/S1383762122000777.

[10] Più diffusamente sulla tecnologia *blockchain*, vedi, in ambito italiano: C. BOMPREZZI, M. PALMIRANI, *Blockchain e smart contract,* in A.M. GAMBINO (a cura di), *Persona e diritti digitali nella smart city*, in G.F. FERRARI (a cura di), *Innovazione e sostenibilità per il futuro delle smart cities*, Milano: Mimesis, 2023, pp. 275-298; S. COMELLINI, M. VASAPOLLO, *Blockchain, criptovalute, I.C.O. e smart contract*, Rimini: Maggioli, 2019; L.M. PERUGINI, *Distributed ledger technologies e sistemi di blockchain: digital currency, smart contract e altre applicazioni*, Milano: Key editore, 2018; M. NICOTRA, F. SARZANA DI SANT'IPPOLITO, *Diritto della blockchain, intelligenza artificiale e IoT*, Milano: Ipsoa, 2018. In ambito internazionale: I. BASHIR, *Mastering blockchain*, Birmingham: Packt, 2018; M. SWAN, *Blockchain, Blueprint for a New Economy*, Sebastopol: O' Reilly, 2015; A. WRIGHT, P. DE FILIPPI, *Decentralized Blockchain Technology and The Rise of Lex Cryptographia*, in *SSRN*, 2015, http://papers.ssrn. com/abstract=2580664.

fatto che le *blockchain permissionless* sono *general purpose* e la loro architettura è creata dall'aggiunta progressiva dei nodi di chiunque voglia accedervi; al contrario, le *blockchain permissioned* sono costruite appositamente per uno scopo predeterminato, sia esso di una singola entità o, ad esempio, di un consorzio, che decidono di investire nella creazione dell'intero sistema *hardware* e *software*[11].

Essendo un database, la *blockchai*n può memorizzare sia il programma informatico che la sua esecuzione nel tempo, secondo il processo decentralizzato e *tamper-resistant* sopra descritto. Ne deriva l'impossibilità unilaterale di apprestare dei cambiamenti nel codice o di arrestarne l'operatività una volta avvenuto il *deployment* in *blockchain*[12]. Per questa ragione, qualora lo *smart contract blockchain-based* venga utilizzato in ambito contrattuale, si è ritenuto che si possa evitare l'inadempimento della parte obbligata alla quale, una volta che lo *smart contract* venga attivato sulla *blockchain*, sarebbe impedito di governare l'esecuzione della propria prestazione, che avverrebbe automaticamente.

2. Smart Contract e Smart Legal Contract

L'espressione "*smart contract*" è stata coniata negli Anni '90 dall'informatico Nick Szabo[13], con cui egli intendeva «*a computerized transaction protocol that executes the terms of a contract*»[14]. Szabo teorizzava di demandare interamente l'attività contrattuale a dei software, ritenuti più affidabili dell'uomo[15]. Al tempo, le teorie di Szabo non erano supportate da una specifica tecnologia[16]. Nel decennio successivo si sono sviluppati dei sistemi informatici in grado di processare termini contrattuali espressi sotto forma di dati informatici. Harry Surden ha denominato tale capacità dei computer di "leggere" clausole contrattuali come "*data-*

[11] Per approfondimenti sulle tipologie di blockchain, si veda EUROPEAN COMMISSION, JOINT RESEARCH CENTRE, *Blockchain Now and Tomorrow – Assessing Multidimensional Impacts of Distributed Ledger Technologies*, 2019, p. 15; G. HILEMAN, M. RAUCHS, *2017 Global Blockchain Benchmarking Study*, in *SSRN*, 2017, p. 20, https://ssrn.com/abstract =3040224.

[12] P. DE FILIPPI, A. WRIGHT, *Blockchchain and the law – the rule of code*, Cambridge: Harvard University Press, 2018, pp. 74-75; R. H. WEBER, *Smart Contracts: Do we need New Legal Rules?,* in A. DE FRANCESCHI, R. SCHULZE (a cura di), *Digital Revolution – New Challenges for Law*, München: Beck Nomos, 2019, pp. 299-312; A. STAZI, *Automazione contrattuale e "contratti intelligenti" – Gli smart contracts nel diritto comparato,* Torino: Giappichelli, 2019.

[13] Per ulteriori informazioni su Nick Szabo, vedi il seguente link: https://en.wikipedia. org/-wiki/Nick_Szabo.

[14] N. SZABO, *Formalizing and Securing Relationships on Public Networks*, *First Monday*, 1997, https://firstmonday.org/ojs/index.php/fm/article/view/548.

[15] K. WERBACH, N. CORNELL, *Contracts Ex Machina*, in *Duke Law Journal*, 2017 (LXVII), pp. 313-382.

[16] M. GIANCASPRO, *Is a 'smart contract' really a smart idea? Insights from a legal perspective*, in *Computer Law & Security Review*, 2017 (XXXIII), pp. 825-835.

oriented contracting"[17]*,* e come "*computable contracts*" la possibilità dei medesimi di sostituire la parte contrattuale[18]. Come affermato dallo stesso Surden, però, con i *computable contract* se le parti non sono soddisfatte dal risultato dell'elaborazione del computer, possono scartarlo. Permangono dunque il monitoraggio e la supervisione umana[19].

Gli *smart contracts* basati su *blockchain*, diversamente, appaiono come la realizzazione concreta di quanto precedentemente immaginato da Nick Szabo. La decentralizzazione e la resistenza alle manomissioni (o immutabilità) della *blockchain* impedirebbero alla parte debitrice di poter influenzare l'esecuzione del contratto una volta che lo *smart contract* sia stato attivato sulla *blockchain*, rendendolo autonomo[20]. Pertanto, si ritiene che la *blockchain* rimuova il bisogno da parte del creditore di fare affidamento sul debitore circa l'adempimento del contratto[21]. Si passerebbe dalla fiducia nella controparte contrattuale umana alla fiducia nel codice[22], potendo così aumentare le *chances* di soddisfare pienamente l'interesse del creditore[23],

In senso contrario, sono state teorizzate svariate situazioni in cui, nonostante la *blockchain*, l'auto-esecuzione di prestazioni per mezzo di *smart contract* non garantirebbe il soddisfacimento della parte creditrice. Volendo tentare una schematizzazione, si potrebbero identificare tre gruppi: a) il codice informatico non è conforme alla volontà delle parti; b) il verificarsi di malfunzionamenti tecnici;

---

[17] H. SURDEN, *Computable Contracts*, in *U. C. Davis Law Review*, 2012 (XLVI), pp. 629-700.

[18] *Ibid.*, p. 658.

[19] K. WERBACH, N. CORNELL, *Contracts Ex Machina*, cit., pp. 322-323.

[20] P. DE FILIPPI, A. WRIGHT, *Blockchchain and the Law – the Rule of Code*, cit., pp. 74-75; R.H. WEBER, *Smart Contracts: Do we need New Legal Rules?*, cit., p. 308; A. STAZI, *Automazione contrattuale e "contratti intelligenti" – Gli smart contracts nel diritto comparato*, cit., p. 100; M. MAUGERI, *Smart contracts e disciplina dei contratti*, Bologna: Il Mulino, 2021, p. 24.

[21] A. SAVELYEV, *Contract law 2.0: 'smart' contracts as the beginning of the end of classic contract law*, in *Higher School of Economics Research Paper no. WP BRP 71/LAW/2016*, 2016, p. 11, https://ssrn.com/abstract=2885241; P. CUCCURU, *Blockchain ed automazione contrattuale, riflessioni sugli smart contract*, cit., p. 107.

[22] T. J. De GRAAF, *From old to new: from internet to smart contracts and from people to smart contracts*, in *Computer Law & Security Review*, 2019 (XXXV), pp. 1-11. L'autore fa l'esempio dello sblocco di un'auto intelligente noleggiabile dietro pagamento mediante apposita *app*. Questi sostiene che, mentre senza *blockchain* il sistema informatico in grado di aprire o chiudere l'auto sarebbe sotto il controllo del noleggiatore, con la *blockchain* quest'ultimo non potrebbe alterarne il funzionamento.

[23] Secondo M. CRISAFULLI, *L'era degli Smart Contracts: potenzialità e limiti di uno strumento rivoluzionario*, in *Diritto Mercato Tecnologia*, 3 giugno 2021, p. 19 «In primo luogo, mediante l'impiego di un processo di esecuzione totalmente automatizzato, è chiaro che, almeno ipoteticamente, si potrà avere una consequenziale diminuzione di liti e dispute collegate alla materia contrattuale. In secondo luogo, come aspetto direttamente correlato al primo, andrebbero a perdere di importanza tutti quegli strumenti di garanzia volti ad assicurare l'adempimento del debitore».

c) il carattere chiuso della blockchain quando l'adempimento del contratto implica forme di interazione con il mondo esterno[24].

La prima ipotesi è facilmente intuibile: quando il codice dello *smart contract* non combacia con quanto voluto dalle parti, indipendentemente dal fatto che l'esecuzione avvenga correttamente sul piano tecnico, sul piano giuridico si configura un inadempimento contrattuale.

Per quanto concerne la seconda, problemi tecnici potrebbero colpire una o più componenti di un'applicazione *blockchain-based*,[25] influendo negativamente sulla corretta esecuzione del contratto. Anzitutto, come ogni programma informatico, lo *smart contract* stesso potrebbe avere dei *bug*[26]. Altre problematiche potrebbero affliggere il protocollo *blockchain* sottostante[27], con conseguenze negative sullo *smart contract ivi* registrato[28]. Anche gli *oracle* – interfacce che trasmet-

---

[24] Tale schematizzazione è proposta da C. BOMPREZZI, *From Trust in the Contracting Party to Trust in the Code in Contract Performance: A Critical Analysis of the Relationship between Blockchain-Based Smart Contracts and Consumer Protection,* in *EuCML*, 2021 (IV), pp. 148-159.

[25] Ogni soluzione *blockchain* potrebbe intendersi come la somma di più livelli, o "*multi-layered*". In estrema sintesi, alla base vi è il *protocol layer*, cioè l'infrastruttura hardware e software del database; su questo si eseguono i software delle varie applicazioni, che costituiscono il livello sovrastante, o *application layer*, dove si trovano anche gli *smart contract*. vedi G. HILEMAN, M. RAUCHS, *2017 Global Blockchain Benchmarking Study*, in *SSRN*, p. 26, https://papers.ssrn.com/sol3/ papers.cfm?abstract_id=3040224. Vi sono svariati *providers* di soluzioni *blockchain*; Vedi J SINGH, J.D MICHELS, *Blockchain as a Service*, in *Queen Mary University of London, School of Law, Legal Studies Research Paper No. 269/2017*, p. 4, https://ssrn.com/abstract=3091223, parlano di "*Blockchain-as-a-Service*" (*BaaS*), *service providers* che offrono e gestiscono varie componenti di un'infrastruttura DLT. Vedi A. DAVOLA, *Blockchain e smart contract as a service: prospettive di mercato e criticità normative delle prestazioni BAAS e SCAAS alla luce di un'incerta qualificazione giuridica*, in *Il Diritto Industriale*, 2020 (II), p. 147, distingue tra *Blockchain as a Service* (*BaaS*) e *Smart Contract as a Service* (*SCaaS*).

[26] A. SAVELYEV, *Contract law 2.0: 'smart' contracts as the beginning of the end of classic contract law*, cit., p. 14; per esempio, nel 2016 Peter Vessenes (co-fondatore della Bitcoin Foundation) ha stimato che gli *smart contract* di Ethereum contenevano 100 errori ogni 1000 linee di codice informatico. Vedi P. VESSENES, *Ethereum Contracts are Going to be Candy for Hackers*, *Vessenes*, 18 maggio 2016, http://vessenes.com/ethereum-contracts-are-going-to-be-candy-for-hackers/.

[27] E. MIK, *Blockchains. A Technology for Decentralized Marketplaces*, in L.A. DI MATTEO *et al.* (a cura di), *The Cambridge Handbook of smart contracts, blockchain technology and digital platforms,* Cambridge: Cambridge University Press, 2020, pp. 160-182. Esse concernono primariamente la selezione e l'ordine delle transazioni. Al riguardo, vedi L. LUU *et al.*, *Making Smart Contracts Smarter*, *ACM SIGSAC Conference on Computer and Communications Security*, Vienna 2016, pp. 254-269, https://doi.org/10.1145/2976749.2978309. Per esempio, il contributo cita la cd "*transaction-ordering dependency*", che si verifica quando più transazioni invocano lo stesso *smart contract*. Ciò può dare risultati inaspettati ad un utente che invoca uno *smart contract* quando ci sono altre transazioni concomitanti, a seconda dell'ordine in cui le transazioni sono validate e aggiunte in *blockchain*. Si immagini, in un contratto di vendita, che il venditore aggiorni il prezzo del bene in vendita al rialzo; l'acquirente potrebbe dover pagare un prezzo più alto di quello che abbia accettato di pagare inviando la propria accettazione, qualora la transazione di aggiornamento del prezzo del venditore si collochi temporalmente prima di quella di accettazione del contratto dell'acquirente.

[28] Riprendendo l'esempio della *transaction-ordering dependency* descritto alla nota che precede, si potrebbe pensare ad un *Puzzle contract* in Ethereum, che ricompensa gli utenti che risolvono un

tono le informazioni da e verso la *blockchain* – potrebbero non funzionare a regola d'arte[29]. Un loro non corretto operare potrebbe minare alla realizzazione del volere contrattuale[30]. Da ultimo, posto che gli *oracle* traggono gli input da inviare allo *smart contract* da fonti esterne di dati è indispensabile che anche queste ultime siano affidabili. Invero, anche le fonti di dati potrebbero essere soggette a malfunzionamenti o inattive[31].

Infine, il terzo gruppo ricomprende i casi in cui l'esecuzione del contratto è inattuabile senza il collegamento tra ciò che si svolge *on-chain* e *off-chain*. Infatti, la *blockchain* è stata definita "*deaf and blind*", non potendo direttamente ricevere informazioni se non quelle ricavabili al suo interno[32] (si pensi, ad esempio, ad un trasferimento di *token* rappresentanti beni nativi di *blockchain* in cambio di un certo ammontare in criptovalute). Da qui l'importanza degli *oracle* e delle fonti esterne di dati, di cui sopra[33]. Dunque, se tali informazioni non vengono trasmesse in modo appropriato o non vengono affatto veicolate, lo *smart contract* non si esegue o non si esegue correttamente, con quanto ne può seguire sul piano dell'adempimento contrattuale. D'altra parte, ciò può accadere non solo a causa di malfunzionamenti tecnici (in tal caso, si ricadrebbe nel secondo gruppo), ma anche per azioni o errori umani. Si immagini la consegna di un'opera d'arte (registrata in *blockchain* mediante apposito NFT) da parte di un trasporta-

---

puzzle computazionale. L'obbligato potrebbe sfruttare il *transaction-ordering*. Vale a dire, questi potrebbe aspettare fino a quando un utente non invii una soluzione corretta del puzzle e inviare immediatamente una transazione che riduca la ricompensa del contratto a zero. Se quest'ultima transazione viene aggiunta in *blockchain* prima di quella dell'utente, questi non ottiene alcuna ricompensa. Un altro esempio è il famigerato "*TheDao hack*" del 2016, dove un hacker è stato in grado di rubare oltre tre milioni di *ethers* (la criptovaluta di Ethereum) utilizzando la cd "*reentrancy vulnerability*". Vedi L. LUU *et al.*, *Making Smart Contracts Smarter*, cit., pp. 257-259.

[29] E. MIK, *Smart contracts: terminology, technical limitations and real world complexity*, in *Journal of Law, Innovation and Technology*, 2017 (IX), pp. 269-300.

[30] Gli *oracle* potrebbero inviare informazioni errate allo *smart contract* (in entrata) o all'esterno della *blockchain* (in uscita).

[31] M. GIANCASPRO, *Is a 'smart contract' really a smart idea? Insights from a legal perspective*, cit., p. 833. Si pensi ad un contratto di assicurazione intelligente programmato per pagare l'assicurato in caso di ritardo di un volo aereo di due ore. Si potrebbe immaginare che il s*oftware* dell'aeroporto che riporta gli orari di arrivo non funzioni per alcune ore, e non registri il ritardo. L'esempio è di M. CLÉMENT, *Smart Contracts and the Courts*, in L.A. Di MATTEO *et al.* (a cura di), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, cit., p. 280.

[32] O. RIKKEN *et al.*, *Smart contracts as a specific application of blockchain technology*, 2017, p. 17, https://dutchdigitaldelta.nl/uploads/pdf/Smart-Contracts-ENG-report.pdf.

[33] A.U. JANSSEN, F.P. PATTI, *Demistificare gli smart contracts*, in *Osservatorio del Diritto Civile e Commerciale*, 2020 (I), pp. 31-50, spec. p. 41: «gli oracles forniscono allo smart contract le informazioni esterne necessarie per l'esecuzione (ad esempio, il prezzo delle azioni o il prezzo dell'oro). È dunque evidente che l'utilizzazione di oracle si pone in contrasto con l'assunto secondo cui gli smart contracts si eseguono automaticamente. Ogni oracle riduce il livello di automazione del contratto, poiché implica uno o più passaggi ulteriori nel processo di esecuzione delle prestazioni».

tore specializzato, che indichi erroneamente di aver condotto il bene a destinazione, mentre quest'ultimo non sia affatto pervenuto all'indirizzo del destinatario, oppure sia difforme da quanto concordato nel contratto.

Sempre a causa della natura chiusa di *blockchain*, l'esecuzione dello *smart contract* potrebbe dover essere accompagnata da altre azioni al di fuori del registro per l'adempimento del contratto. Riprendendo l'esempio fatto pocanzi dell'opera d'arte, si pensi alla prestazione di consegna fisica del bene.

3. Smart Contract e Data Act

Il Regolamento europeo sui dati, meglio conosciuto come *Data Act*,[34] fa parte degli atti legislativi dell'Unione europea che rientrano nella "Strategia europea in materia di dati",[35] il cui obiettivo è quello di creare un mercato unico in cui i dati possano circolare liberamente nello spazio europeo, a beneficio di cittadini, imprese e pubbliche amministrazioni, con regole chiare ed eque. In particolare, con il *Data Act* si mira a rendere disponibile per l'uso un maggior numero di dati e a stabilire norme su chi può utilizzarli e accedervi e per quali scopi in tutti i settori economici dell'UE.

Su questo, gli *smart contract* acquisiscono un ruolo centrale, potendo fornire ai titolari e ai destinatari dei dati garanzie del rispetto degli accordi di condivisione dei dati[36]. Infatti, al considerando 47 il *Data Act* suggerisce l'uso di contratti intelligenti per gestire accordi a lungo termine tra i titolari e i destinatari dei dati, al fine di ridurre i costi in operazioni regolari e ripetitive nell'ambito di una relazione commerciale. Inoltre, i contratti intelligenti sono citati tra le adeguate misure tecniche di protezione che il titolare dei dati può applicare per impedire l'accesso non autorizzato ai dati (v. art. 11).

Oltre che suggerire il ricorso a contratti intelligenti per gestire le condizioni di accesso e condivisione dei dati, il *Data Act* si occupa, altresì, di fornire una definizione di "contratto intelligente"[37] e di stabilire i requisiti essenziali che tali

---

[34] Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio, del 13 dicembre 2023, riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (regolamento sui dati), GU L, 2023/2854, 22.12.2023, pp. 1-71.

[35] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-f it--digital-age/european-data-strategy_it.

[36] EU BLOCKCHAIN OBSERVATORY AND FORUM, *Smart Contracts*, 4 November 2022, p. 20, https://blockchain-observatory.ec.europa.eu/publications/smart-contracts_en).

[37] Ai sensi dell'art. 2, par. 1, n. 39, un "contratto intelligente" è «un programma informatico utilizzato per l'esecuzione automatica di un accordo o di parte di esso utilizzando una sequenza di registrazioni elettroniche di dati e garantendone l'integrità e l'accuratezza del loro ordine cronologico».

contratti intelligenti devono avere per essere utilizzati per l'esecuzione degli accordi di condivisione dei dati succitati[38].

Coerentemente a quanto già ribadito, i contratti intelligenti non sono necessariamente legati alla *blockchain*, essendo la nozione di contratto intelligente *ivi* fornita tecnologicamente neutra[39]. Ma, come esplicitato al considerando 104 del regolamento in esame, "*i contratti intelligenti possono ad esempio essere collegati a un registro elettronico*". La locuzione di registro elettronico si ricava dal nuovo Regolamento eIDAS, con un chiaro riferimento alla *blockchain*, su cui si veda *infra*.

4. Blockchain e Regolamento eIDAS

Il recente Regolamento UE n. 1183 del 2024[40], di modifica del Regolamento UE n. 910 del 2014 altrimenti conosciuto come Regolamento eIDAS (da cui il riferimento al regolamento di modifica come eIDAS 2) ha previsto, tra i nuovi servizi fiduciari, il registro elettronico, definito quale «una sequenza di registrazioni di dati elettronici che garantisce l'integrità di tali registrazioni e l'accuratezza dell'ordine cronologico di tali registrazioni» (art. 3, punto 52). L'art. 45 *duodecies*, nel suo primo paragrafo, contrasta la negazione di effetti giuridici ai registri elettronici e l'ammissibilità come prova unicamente per via della forma elettronica[41]. Dalla lettura congiunta del primo e del secondo paragrafo dell'art. 45 *duodecies* emerge poi una suddivisione tra registri elettronici semplici e registri elettronici qualificati, quest'ultimo inteso come «un registro elettronico fornito da un prestatore di servizi fiduciari qualificato e che soddisfa i requisiti di cui all'articolo 45 terdecies» (art. 3, par. 1, n. 53). Le due tipologie si differenziano dal punto di vista dell'effetto giuridico. Più precisamente, l'articolo non disciplina gli effetti giuridici del registro elettronico semplice, ma questi ultimi possono dedursi da quanto disposto per i registri elettronici qualificati, per i quali si presume l'ordine cronologico sequenziale univoco e l'integrità dei dati in

[38] Ai sensi dell'art. 36, i requisiti essenziali sono: robustezza e controllo dell'accesso; cessazione e interruzione sicure; archiviazione e continuità dei dati; controllo dell'accesso; coerenza. La conformità ai requisiti essenziali è presunta nei casi previsti ai paragrafi successivi dell'art. 36. Ai sensi della Proposta Digital Omnibus (COM(2025) 837 final del 19/11/2025) l'art. 36 verrebbe soppresso per evitare difficoltà sul piano dei costi e delle opportunità nei confronti degli innovatori. La soppressione "*promuoverebbe pertanto lo sviluppo e l'introduzione sul mercato di nuovi modelli di business, favorirebbe l'innovazione e ridurrebbe gli ostacoli per le tecnologie emergenti*" (v. cons. 16).

[39] Vedi cons. 104.

[40] Regolamento (Ue) 2024/1183 del Parlamento europeo e del Consiglio dell'11 aprile 2024 che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale, GU L, 2024/1183, 30.04.2024, pp. 1-56.

[41] In ossequio al principio di non discriminazione, elaborato originariamente in seno all'UNCITRAL e adottato nel Model Law on electronic Commerce del 1996, nel Model Law on Electronic Signatures del 2001 e nella Convention on the Use of Electronic Communications in International Contracts del 2005, nonché trasposto nel Regolamento eIDAS.

essi contenuti. La presunzione viene fatta valere mediante la dimostrazione del raggiungimento dei requisiti propri di un registro elettronico qualificato (elencati al successivo art. 45 *terdecies*)[42]. Viceversa, in caso di registro elettronico semplice varrà la valutazione discrezionale del giudice. Un registro elettronico qualificato è riconosciuto come tale, secondo il principio del mutuo riconoscimento, in tutti gli altri Stati membri (art. 24-*bis*, n. 11).

Il Regolamento eIDAS 2 riconosce a livello europeo effetti giuridici alla *blockchain*. L'utilizzo dell'espressione "registro elettronico" è chiaramente ispirata al principio della neutralità tecnologica. In futuro, infatti, potrebbero nascere tecnologie diverse dalla *blockchain*, seppur con le medesime caratteristiche, con il rischio di non trovare una copertura normativa. Oltretutto, esistono già sistemi distribuiti alternativi alla *blockchain*, ma sprovvisti dell'usuale raggruppamento delle transazioni di dati in blocchi, i quali vengono erroneamente denominati *blockchain* poiché in grado di fornire le stesse funzionalità. Il rispetto del principio della neutralità tecnologica, invece, rende la disciplina adatta agli sviluppi e alle varianti future, in questo campo presumibilmente molto plausibili e rapidi data la giovinezza della tecnologia.

Dall'analisi di questi articoli si desume che il legislatore europeo intende accostare alla *blockchain* effetti giuridici più ampi della mera validazione temporale elettronica[43], da cui va distinta[44].

L'art. 8-*ter* della Legge n. 12 dell'11 febbraio 2019, di conversione del decreto legge 14 dicembre 2018, n. 135, rubricato "Tecnologie basate su registri distribuiti e smart contract", fornisce una definizione di tecnologie basate su registri distribuiti e di *smart contracts*, a cui riconosce determinati effetti giuridici. La norma, che è già stata oggetto di molte critiche[45], appare per buona parte in contrasto con le previsioni del Reg. eIDAS 2 sui registri elettronici.

---

[42] La Commissione europea entro il 21 maggio 2025 stabilisce mediante atti di esecuzione un elenco di norme di riferimento e, se necessario, specifiche e procedure applicabili ai requisiti prescritti per i registri elettronici qualificati, secondo la classica procedura prescritta all'articolo 48, par. 2, del Regolamento. La rispondenza dei registri elettronici alle norme, alle specifiche e alle procedure di cui agli atti d'esecuzione della Commissione ammette di poter presumere il rispetto dei requisiti elencati all'art. 45 *terdecies*, par. 1 (vedi art. 45 *terdecies*, par. 2 e 3).

[43] C. BOMPREZZI, *Nuovo eIDAS e registri elettronici: regole e impatti per i servizi fiduciari*, *AgendaDigitale.eu*, 9 settembre 2021, https://www.agendadigitale. eu/documenti/nuovo-eidas-e-registri-elettronici-le-nuove-regole-e-gli-impatti-per-i-servizi-fiduciari/.

[44] Vedi cons. 68 Reg. eIDAS 2.

[45] Vedi S. RIGAZIO, *Smart contracts e tecnologie basate su registri distribuiti nella L. 12/2019*, in *Dir. Inf. Inf.*, 2021(II), pp. 369-395; G. REMOTTI, *Blockchain smart contract. Un primo inquadramento*, in *Oss. dir. civ. e comm.*, 2020 (I), pp. 189-228; G. FINOCCHIARO, *Intelligenza artificiale e protezione dei dati personali*, in *Giurisprudenza Italiana*, 2019 (VII), pp. 1670-1677; M. MANENTE, *L. 12/2019 – Smart contract e tecnologie basate su registri distribuiti – prime note*, Studio 1_2019, Marzo 2019, p. 6, https://www.notariato.itit.ufficio_studi/studio-12019-di-legge-122019-smart-contract-e tecnolo-

A mente del comma 1 dell'art. 8-*ter*, sono "tecnologie basate su registri distribuiti" *quelle* «tecnologie e protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili». La definizione rimanda evidentemente alle cosiddette "*distributed ledger technologies*" (o DLT), e dunque si riferisce ad una tecnologia specifica, di cui esplicita alcune caratteristiche tecniche, contrariamente alla scelta del legislatore europeo di sposare il principio di neutralità tecnologica sia nella denominazione che nella descrizione del *database*.

Il comma 3, poi, sancisce che «la memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui all'articolo 41». La validazione temporale elettronica, secondo la definizione dell'art. 3, par. 1, n. 33 del Regolamento eIDAS consente di accostare data e ora a dati in forma elettronica ad opera di altri dati in forma elettronica, al fine di provare l'esistenza dei medesimi in un determinato momento. Sinonimo di validazione temporale è l'utilizzo dell'espressione "marca temporale" (o "*timestamp*"), che normalmente viene effettuata mediante funzioni di "*hash*" in grado di generare un'impronta digitale univoca dei dati da validare.

Nel menzionare la validazione temporale elettronica, il comma 3 rimanda all'art. 41 del Regolamento eIDAS, che disciplina gli effetti giuridici della validazione temporale elettronica. In particolare, se la validazione temporale elettronica è qualificata (e cioè soddisfa determinati requisiti elencati all'art. 42 Reg.), essa gode della presunzione di accuratezza della data e dell'ora indicate e dell'integrità dei dati a cui data ed ora sono associate; in caso contrario, tale valutazione è rimessa al libero apprezzamento del giudice. Il quarto comma della legge italiana subordina la produzione degli effetti giuridici della validazione temporale all'individuazione di determinati *standard* tecnici elaborati dall'Agenzia per l'Italia digitale.

Ad ogni buon conto, il carattere obbligatorio e direttamente applicabile dello strumento del regolamento impone allo Stato italiano di adeguare il proprio or-

---

gie-basate-suregistridistribuiti ; C. BOMPREZZI, *Commento in materia di Blockchain e Smart contract alla luce del nuovo Decreto Semplificazioni*, in *Diritto Mercato Tecnologia*, 2019, https://www.dimt.it/news/breve-commento-alla-legge-11-febbraio-2019-n-12-di-conversionedel-decreto-legge-14-dicembre-2018-n-135-recante-disposizioni-urgenti-in-materia-di-sostegno-esemplificazione-per-le-i mprese-e-per-la-pu/.

dinamento. In ogni caso, la mancata adozione di *standard* tecnici e linee guida da parte di AGID rende la disciplina italiana sostanzialmente inapplicata.

Un altro punto di contatto tra *blockchain* e regolamento eIDAS è la possibilità di qualificare come documento informatico ogni dato e/o informazione inseriti in *blockchain*, *smart contract* compresi. A ribadirlo è uno studio dell'EU Blockchain Observatory and Forum del 2019[46], per quanto ciò si possa ricavare immediatamente in via interpretativa. Ai sensi dell'eIDAS, infatti, il documento elettronico è «qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva» (art. 3, par. 1, n. 35)[47].

5. Blockchain e protezione dei dati personali

Nell'ambito della protezione dei dati personali, sono stati colti degli aspetti della tecnologia *blockchain* che potrebbero contribuire a raggiungere gli obiettivi posti dal GDPR e che potrebbero dunque rappresentare un'opportunità per la protezione dei dati personali degli utenti. Nella Dichiarazione istitutiva della *Blockchain Partnership* Europea[48] si è affermato che i servizi *blockchain-based* aiuteranno a preservare l'integrità dei dati e garantiranno una migliore gestione dei dati medesimi da parte dei cittadini e delle organizzazioni che interagiscono con le pubbliche amministrazioni. Il Parlamento europeo, in una Risoluzione del 3 ottobre 2018 ha dichiarato che la *blockchain* «può costituire uno strumento che rafforza l'autonomia dei cittadini dando loro l'opportunità di controllare i propri dati e decidere quali condividere nel registro, nonché la capacità di scegliere chi possa vedere tali dati»[49].

---

[46] EU BLOCKCHAIN OBSERVATORY AND FORUM, *Legal and Regulatory Framework of Blockchains and Smart Contracts*, cit., p. 21.

[47] Parimenti, ai sensi del Codice dell'Amministrazione Digitale (D.Lgs. 82/2005, o CAD) il documento informatico è in il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti» (art. 1, 1° co., lett. p). Anche a livello internazionale, peraltro, le leggi *ad hoc* di California (California Assembly Bill 2658 https://legiscan.com/CA/text/AB2658/id/1732549), Tennessee (Tennessee Senate Bill No. 1662 https://legiscan.com/TN/text/SB 1662/2017) e Arizona (Arizona House Bill No. 2417 https://www.azleg.gov/legtext/ 53leg/1R/laws/0097.htm), esplicitamente accostano ad ogni *record* in *blockchain* la denominazione di "*electronic record*".

[48] Iniziativa che ha coinvolto 30 Stati europei per collaborare sul tema (https://digital-strategy.ec.europa.eu/en/policies/blockchain-partnership).

[49] Risoluzione del Parlamento europeo del 3 ottobre 2018 sulle tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione (2017/2772\(RSP)), considerando A.

Capacità di tenuta sicura, trasparente e tracciabile dei dati, accesso e condivisione selettivi sarebbero in linea con alcuni importanti principi del GDPR, quali il principio di *privacy by design*[50], di trasparenza[51] o di minimizzazione[52].

D'altra parte, non mancano elementi di frizione tra la tecnologia *blockchain* e la normativa europea a tutela dei dati personali.

Una delle domande più ricorrenti tra gli esperti è se sia individuabile un titolare del trattamento[53] e, in caso affermativo, chi possa essere considerato tale, in presenza di applicazioni decentralizzate che colliderebbero con la visione centralizzata e gerarchica che accompagna il GDPR. Le maggiori difficoltà interessano le *blockchain* di tipo *permissionless*, in assenza di un'entità deputata a governare il sistema e ad assumere decisioni strategiche, e in cui i nodi sono uguali tra loro, senza limitazioni d'accesso, senza preidentificazione, senza predeterminazione a monte degli usi (e quindi delle finalità) per cui la *blockchain* è stata concepita.

---

[50] Art. 25 GDPR, per cui il titolare del trattamento deve mettere in atto «misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente Regolamento e a tutelare i diritti degli interessati».

[51] Art. 5, par. 1, lett. a GDPR, ai sensi del quale i dati personali sono trattati «in modo lecito, corretto e trasparente nei confronti dell'interessato».

[52] Art. 5, par. 1, lett. c GDPR, che richiede che i dati siano «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati». Su questi aspetti, si veda A.M. GAMBINO, C. BOMPREZZI, *Blockchain e protezione dei dati personali*, in *Dir. Inf. Inf.*, 2019 (III), pp. 619-646. Più in generale, sul rapporto tra *blockchain* e protezione dei dati personali, vedi G. D'ACQUISTO, *Blockchain e GDPR: verso un approccio basato sul rischio*, in *Federalismi.it*, 2021 (II), pp. 53-65; U. TATAR *et al.*, *Law versus technology: Blockchain, GDPR, and tough tradeoffs*, in *Computer Law & Security Review*, 2020 (XXXVIII), pp. 1-11; F. FAINI, *Blockchain e diritto: la "catena del valore" tra documenti informatici, smart contracts e data* protection, in *Resp. civ. e prev.*, 2020 (I), pp. 297-316; M. FINCK, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?*, https://www.europarl.europa.eu/RegData/etudes/STUD/ 2019/634445/ EPRS_STU(2019)634445_EN.pdf; ID., *Blockchain regulation and Governance in Europe*, Cambridge: Cambridge University Press, 2018; ID., *Blockchains and Data Protection in the European Union*, *Max Planck Institute for Innovation and Competition Research Paper n. 18-01*; A.M. GAMBINO, C. BOMPREZZI, *Circolazione e protezione dei dati nella blockchain*, in A M. GAMBINO, A. STAZI (a cura di), *La circolazione dei dati – Titolarità, strumenti negoziali, diritti e tutele*, Pisa: Pacini, 2020, pp. 213-240; T. LYONS *et al.*, *Blockchain and the GDPR – a Thematic Report Prepared by the European Union Blockchain Observatory and Forum*, 16 ottobre 2018, https://www.eublockchain forum.eu/reports; M. BERBERICH, M. STEINER, *Blockchain technology and the GDPR – How to Reconcile Privacy and Distributed Leers?*, in *European Data Protection Law Review*, 2016 (II), pp. 422-426; L. D. IBÁÑEZ *et al.*, *On Blockchains and the General Data Protection Regulation*, https://eprints.soton.ac .uk/422879/1/Block chains_GDPR _4.pdf; P. DE FILIPPI, *The interplay between decentralization and privacy: the case of blockchain technologies*, in *SSRN*, 2016, https://ssrn.com/abstract=2852689.

[53] Ai sensi dell'art. 4, par. 1, n. 7 del GDPR, il titolare del trattamento è la persona fisica o giuridica che determina le finalità (il perché) e i mezzi (il come) del trattamento. Questi assume la responsabilità dell'osservanza delle norme a protezione dei dati personali nei confronti dei soggetti (interessati) i cui dati personali sono oggetto di trattamento da parte del titolare.

Le ricostruzioni in proposito sono varie. Tra le più accreditate quella che attribuirebbe il ruolo di titolare ai singoli nodi (o meglio, ai singoli *user*[54]) del sistema, che si siano avvalsi dell'infrastruttura *blockchain* per un particolare scopo.

Anche qualora l'identificazione del titolare del trattamento sia astrattamente possibile, e si avvalori la tesi più condivisa sopra esposta, rimarrebbe arduo per il titolare poter monitorare e governare la gestione dei dati inseriti; l'ostacolo starebbe, cioè, nell'incontrollata duplicazione dei dati personali in nodi detenuti in luoghi e da soggetti non identificabili, in netto contrasto con i dettami delle più importanti norme del GDPR, primo tra tutti il principio di *accountability*[55].

Oggetto di dibattito è anche la presunta incompatibilità tra l'immutabilità di *blockchain* e alcuni principi e diritti che richiederebbero interventi successivi sul *database*, come il principio di limitazione della conservazione[56], il diritto di cancellazione[57] o di rettifica[58]. Circa le soluzioni avanzate sul piano legale, la più plausibile sembra quella che intende la non disponibilità del dato non come distruzione fisica di esso, ma come inaccessibilità tecnica, attraverso varie modalità (come lo storage di dati *off-chain*, la distruzione della chiave privata, l'aggiunta di transazioni che annullino o correggano le precedenti, etc.). Rimane poi l'opzione tecnica di concepire *blockchain* editabili, come i *chameleon hashes*, che consentirebbero la modifica dell'*hash* pur non alterando quelli immediatamente successivi che compongono la catena di blocchi.

Un altro interrogativo attiene alla possibilità di parlare di trasferimento dei dati personali[59] a fronte dell'operazione di replica delle copie di *blockchain* in nodi all'infuori dei confini europei. Si è avanzato sul punto un parallelismo con la sentenza *Bodil Lindqvist* della Corte di Giustizia Europea[60]. che ha negato che

---

[54] I nodi sarebbero semplicemente le componenti tecnologiche dell'infrastruttura, mentre gli *users* sarebbero i soggetti che, mediante collegamento ai nodi, inseriscono le transazioni.

[55] Il principio di *accountability* sta ad indicare la responsabilità che incombe sul titolare del trattamento e abbraccia una concezione del rischio che non è limitata alla fase della violazione, ma che si estende anche a quella precedente, in cui il dato non è stato violato ma potrebbe esserlo sulla base di determinati rischi che spetta al medesimo valutare, approntando tutta una serie di accorgimenti in via cautelativa. Problemi non si porrebbero con *blockchain permissioned*, che di fatto replicano un modello di *governance* centralizzato. Problemi non si porrebbero con *blockchain permissioned*, che di fatto replicano un modello di *governance* centralizzato.

[56] Art. 5, par.1, lett. e GDPR: i dati vanno «conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati».

[57] Art. 17 GDPR.

[58] Art. 16 GDPR.

[59] Il GDPR non fornisce una definizione di "trasferimento", la quale è stata perciò elaborata per differenza rispetto al concetto di "comunicazione": con il secondo, si intendono gli spostamenti di dati tra titolari, all'interno dell'Unione; con il primo, i movimenti di dati tra soggetti, titolari o responsabili, purché uno di essi localizzato fuori dai confini europei.

[60] Corte UE, 6 novembre 2003, C- 101/01 *Lindqvist*.

l'inserimento di dati personali in un sito web potesse essere qualificato come "trasferimento" per il fatto che al medesimo possono avere accesso destinatari situati al di fuori dell'Unione europea, perché «i dati personali che giungono al computer di una persona che si trova in un paese terzo, provenienti da una persona che li ha caricati su un sito Internet, non sono stati trasferiti direttamente tra queste due persone, ma attraverso l'infrastruttura informatica del fornitore di servizi di ospitalità presso il quale la pagina è caricata». Il ragionamento potrebbe essere esteso alla *blockchain*. Infatti, in *blockchain* gli *user* possono accedere ai dati contenuti nei blocchi, dai vari nodi in cui la *blockchain* è replicata, i quali potrebbero essere situati anche in Paesi terzi. Anche qui, i dati non sono trasferiti direttamente, ma all'esito di un processo di validazione e successiva replica nei nodi della *blockchain*. Anche qualora si discorra di trasferimento in senso affermativo, comunque, si discute la fattibilità di una conformità con le disposizioni del GDPR corrispondenti[61]. È stato infatti osservato che nelle *blockchain permissionless* i destinatari del trasferimento e la loro collocazione sono sconosciuti. In aggiunta, anche la possibilità di identificare un titolare del trattamento sarebbe dubbia. In assenza di questi elementi, l'assicurazione di un adeguato livello di protezione dei dati personali sarebbe preclusa.

Volendo fare un bilancio, un'inconciliabilità assoluta sarebbe da escludere, trattandosi peraltro di conclusione che arresterebbe il progresso tecnologico e il mercato di riferimento. Semmai, è stato suggerito un approccio caso per caso, tenuto anche conto del fatto che esistono più tipologie di *blockchain* e che le stesse sono diversamente modulabili a seconda della singola applicazione[62]. Le maggiori problematiche si riscontrano comunque innanzi a *blockchain permissionless*, su cui si dovrebbe dunque evitare di far ricadere la scelta[63]-

---

[61] Art. 44 ss. GDPR. Secondo la disciplina sul trasferimento, il trasferimento di dati personali è ammesso se la Commissione europea ha deciso che il luogo in cui il trasferimento è effettuato garantisce un livello di protezione adeguato (art. 45 GDPR). In assenza di una decisione in tal senso della Commissione europea, il trasferimento è consentito solo se il titolare o il responsabile del trattamento hanno fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi (Art. 46 GDPR).

[62] Secondo T. LYONS *et al.*, *Blockchain and the GDPR – a thematic report prepared by the European Union Blockchain Observatory and Forum*, cit., p. 16: «*GDPR compliance is not about the technology, but it is about how the technology is used (…).There is no such thing as a GDPR-compliant blockchain technology. There are only GDPR-compliant use cases and applications*».

[63] Lo studio condotto per lo European Parliamentary Research Service da M. FINCK, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?*, cit., suggerisce tre *policies*: l'elaborazione di specifiche linee guida da parte del Comitato europeo per la protezione dei dati, in maniera coordinata con le autorità di controllo nazionali; il ricorso a certificazioni e codici di condotta; la promozione di una ricerca interdisciplinare.

Nell'aprile del 2025, il Comitato Europeo per la Protezione dei Dati (EDPB) ha adottato delle Linee guida sul trattamento dei dati personali attraverso le tecnologie blockchain[64]. Le linee guida sottolineano l'importanza di implementare misure tecniche e organizzative fin dalle prime fasi della progettazione del trattamento. L'EDPB chiarisce anche che i ruoli e le responsabilità dei diversi attori coinvolti nel trattamento dei dati personali tramite blockchain devono essere valutati durante la fase di progettazione. Inoltre, le organizzazioni dovrebbero effettuare una Valutazione d'Impatto sulla Protezione dei Dati (DPIA) prima di trattare dati personali tramite tecnologie blockchain, soprattutto se il trattamento potrebbe comportare un alto rischio per i diritti e le libertà delle persone. Secondo il Comitato, le organizzazioni dovrebbero anche garantire la massima protezione dei dati personali degli individui durante il trattamento, affinché questi dati non siano accessibili di default a un numero indefinito di persone. Le linee guida forniscono esempi di diverse tecniche di minimizzazione dei dati, così come di gestione e conservazione dei dati personali. In generale, si dovrebbe evitare di memorizzare dati personali in una blockchain se ciò contrasta con i principi della protezione dei dati. Infine, il Comitato evidenzia l'importanza dei diritti degli individui, in particolare riguardo alla trasparenza, alla rettifica e alla cancellazione dei dati personali.

6. Smart contract, Nft e metaverso

Oltre le criptovalute, che costituiscono il primo caso d'uso legato alla tecnologia *blockchain* come mezzo di pagamento alternativo al contante (es. *bitcoins*)[65], attualmente possono rinvenirsi risorse digitali sotto forma di "gettoni digitali", o "*tokens*", i quali possono rappresentare potenzialmente ogni diritto o bene, o della realtà (materiale e immateriale) o "*blockchain* nativi", in quanto originatisi nella stessa *blockchain*[66] (come la cd "*crypto art*")[67]. Tali *tokens* traggono vantaggio dalle caratteristiche della *blockchain*, sopra descritte, divenendo anch'essi, come

[64] EUROPEAN DATA PROTECTION BOARD, *Guidelines 02/2025 on processing of personal data through blockchain technologies*, https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-022025-processing-personal-data_en.

[65] Su cui si rimanda a A.M. GAMBINO, C. BOMPREZZI, *Blockchain e criptovalute*, in G. FINOCCHIARO, V. FALCE (a cura di), *Fintech: diritti, concorrenza, regole – Le operazioni di finanziamento tecnologico*, Bologna: Zanichelli, 2019, pp. 267-290.

[66] C. BOMPREZZI, *Implications of Blockchain-Based Smart Contracts on Contract Law*, Baden Baden: Nomos, 2021, p. 44.

[67] Opere d'arte digitale pubblicate direttamente su *blockchain*.

qualunque informazione registrata all'interno del *database*, unici, inalterabili, non riproducibili, non falsificabili e irrevocabilmente trasferibili[68].

A seconda della funzione, i *token* vengono intesi o come mezzo di pagamento (*crypto-currency*), o come mezzo di speculazione finanziaria (*security token*) o come mezzo di accesso a un bene o un diritto (*utility token*). A parità di strumento tecnologico, cioè, si ha una diversa qualificazione giuridica, con esiti divergenti circa le norme di riferimento. Recentemente, a livello europeo, con il Regolamento del Parlamento europeo e del Consiglio relativo ai mercati delle criptoattività (*Markets in Crypto-Assets* o MiCA)[69] è stato fornito un quadro normativo d'insieme sulle criptoattività, definite come «una rappresentazione di un valore o di un diritto che può essere trasferito o memorizzato elettronicamente, utilizzando la tecnologia di registro distribuito o una tecnologia analoga», con esclusione di quelle che rientrano già nella definizione di strumenti finanziari (da assoggettare alla disciplina corrispondente)[70] e degli NFT[71].

Quest'ultimo acronimo sta per "*Non-Fungible Tokens*", ovvero *token* che, in ragione dei metadati contenuti, sono tecnologicamente non interscambiabili con altri *token* della stessa tipologia, da cui si differenziano divenendo unici (da qui l'aggettivo "infungibili")[72].

Gli *smart contract* permettono la "programmabilità" dei *token*[73], potendo automatizzare le operazioni previste dal codice e attinenti al trasferimento, al ricorrere di condizioni stabilite *ex ante*, del *token* medesimo, o all'esercizio di altre azioni connesse al *token*.

L'associazione *smart contract*/*token* assume rilevanza giuridica laddove il *token*, anche non fungibile, rappresenti beni o diritti di cui disporre mediante *smart contract*. Da questo punto di vista, si può ipotizzare o che lo *smart contract* predetermini le condizioni per il trasferimento del *token* medesimo, o che consenta la

---

[68] EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM, *Regulatory Framework of Blockchains and Smart Contracts*, cit., p. 26.

[69] Regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio, del 31 maggio 2023, relativo ai mercati delle cripto-attività e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937, GU L 150 del 9.6.2023, pagg. 40–205. Il 13 settembre 2024 è stato pubblicato sulla Gazzetta Ufficiale il decreto legislativo 5 settembre 2024, n. 129, recante "Adeguamento della normativa nazionale al regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio, del 31 maggio 2023, relativo ai mercati delle cripto-attivita' e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937".

[70] Vedi cons. 9.

[71] Vedi cons. 10.

[72] Vedi EUROPEAN BLOCKCHAIN OBSERVATORY AND FORUM, *Demystifying Non-Fungible Tokens (NFTs)*, 29 novembre 2021, p. 27, https://www.eublockchainfo rum.eu/reports.

[73] EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM, *Legal and Regulatory Framework of Blockchains and Smart Contracts*, cit., p. 26. La piattaforma *blockchain* Ethereum è la più utilizzata in ambito NFT con il noto standard ERC-721.

gestione dei diritti connessi al *token*. Ad esempio, nella prima fattispecie potrebbe ricadere il passaggio nella titolarità di un bene (rappresentato digitalmente da un NFT). La seconda potrebbe comprendere il caso di *asset* di tipo finanziario, come azioni, che pagano automaticamente i dividendi[74].

Lo *smart contract* potrebbe anche presupporre, come spesso accade, un rapporto contrattuale, in base al quale viene effettuato lo scambio di *tokens* o sono definiti i termini dei diritti relativi al *token*. Si pensi ad uno scambio di libri antichi con criptovalute, in cui il trasferimento è un effetto della conclusione dello *smart legal contract* e la controprestazione in criptovalute un obbligo del soggetto ricevente i libri, oppure alla gestione delle *royalties* connesse ad un'opera soggetta al diritto d'autore riprodotta come NFT[75].

Queste applicazioni si rivelano imprescindibili nel metaverso, in quanto consentono di riproporre, in chiave dematerializzata, le azioni che si effettuerebbero nel mondo fisico nelle interazioni quotidiane ad opera degli utenti, interagenti nel Metaverso sottoforma di *avatars*.

Altresì, la *blockchain* è ampiamente riconosciuta come una tecnologia fondamentale nell'ambito del metaverso, in quanto *database* in cui registrare in modalità sicura, tracciabile, incorruttibile e trasparente le molteplici transazioni che hanno luogo negli ambienti virtuali[76]. Tale convinzione proviene dall'analisi di alcune caratteristiche tecniche della tecnologia in esame[77].

In primo luogo, il fatto che essa faccia parte dei sistemi distribuiti contribuisce alla ridondanza dei dati; più nel dettaglio, la disattivazione di un nodo della rete per un qualsiasi motivo (come, appunto, un attacco alla cibersicurezza) non causa la perdita dei dati che sono detenuti nelle altre copie identiche della stessa catena in altri nodi. Pertanto, la *blockchain* garantisce la disponibilità dei dati in un qualsiasi momento, con la permanente accessibilità da qualsiasi punto del metaverso e, potenzialmente, anche da mondi virtuali diversi.

Oltre alla distribuzione, il carattere decentralizzato della *blockchain*, che implica l'aggiornamento delle informazioni del *database* a partire da un meccani-

---

[74] EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM, *Legal and Regulatory Framework of Blockchains and Smart Contracts*, cit., p. 26.

[75] Come indicato da G. FREZZA, *Blockchain, autenticazione e arte contemporanea*, in *Dir. di Famiglia e delle Persone*, vol. 2020 (II), pp. 491-515.

[76] EU BLOCKCHAIN OBSERVATORY AND FORUM, *Trend Report of Virtual Worlds (Metaverse)*, 24 May 2024, https://blockchain-observatory.ec.europa.eu/publications/ trend-report-virtual-worlds-metaverse_en.

[77] Vedi EU BLOCKCHAIN OBSERVATORY AND FORUM, *Trend Report of Virtual Worlds (Metaverse)*, cit.; K. GOLDSTEIN, *Blockchain and distributed ledger technology: insurance applications, legal development, and cybersecurity considerations*, in *Connecticut Insurance Law Journal*, 2021 (XXVII), pp. 105-122; C. CATALINI, *Blockchain Technology and Cryptocurrencies: Implications for the Digital Economy, Cybersecurity, and* Government, in *Georgetown Journal of International Affairs*, 2018 (XIX) pp. 36-42.

smo del consenso *peer-to-peer*, e non da un punto centrale, diminuisce la vulnerabilità dell'intero impianto a manipolazioni di vario genere. Inoltre, l'immutabilità amplifica le misure di sicurezza. Infatti, l'alterazione dei dati sarebbe possibile solamente modificando in contemporanea l'*hash* del blocco oggetto di attacco, quelli successivi, e tutte le relative copie, prima dell'aggiunta di un nuovo blocco. Questa operazione richiederebbe una potenza e una velocità di calcolo enormi, con costi esorbitanti rispetto all'obiettivo di aprire falle di sicurezza.

La modalità di concatenazione dei blocchi, peraltro, fornisce quella tracciabilità e trasparenza utili a vagliare qualsiasi informazione registrata *on-chain*, dal suo punto di origine alla storia di tutte le transazioni ad essa connesse, aiutando a rilevare eventuali informazioni false o manipolate.

Distribuzione, decentralizzazione, immutabilità, tracciabilità e trasparenza sono qualità preziose in ambiti complessi e variegati come il metaverso, in cui è fondamentale una gestione attenta e oculata di una smisurata quantità di dati continuamente scambiati tra plurimi soggetti, piattaforme, oggetti dell'IoT, *etc.* Non a caso, la *blockchain* si è diffusa principalmente, e sta avendo il maggior successo e riscontro pratico, in settori in cui quotidianamente avviene la condivisione di una molteplicità di dati tra una eterogeneità di attori, e in cui per questo è cruciale mantenere un elevato livello di affidabilità, accortezza, riduzione di errori di duplicazione dei dati e delle tempistiche di condivisione e scambio dei medesimi. In altri termini, uno strumento affidabile, trasparente e tracciabile come la *blockchain* si rivela particolarmente prezioso in una dimensione virtuale i cui gli utenti devono fidarsi che i loro beni virtuali e le operazioni ad essi connessi si trovino un ambiente sicuro[78].

7. Blockchain e self-sovereign identity

La presenza umana nell'ambiente digitale espone a significativi rischi per la protezione dell'identità dell'individuo e della sua sfera privata. È sempre più urgente, dunque, intervenire normativamente affinché si possa garantire uno spazio virtuale sicuro, protetto contro i pericoli legati, ad esempio, all'utilizzo illecito a fini di profitto, alla sorveglianza di massa, alla manipolazione, alle discriminazioni, ai furti di identità, cibersicurezza, alla criminalità informatica, etc. A questo fine, sul piano europeo e internazionale si sta procedendo verso la creazione di identità digitali uniche e sicure, sotto l'esclusivo controllo degli utenti, come alternativa al sistema attuale in cui sono i fornitori a rendere disponibili

[78] EU COMMISSION, JOINT RESEARCH CENTRE, *Next Generation Virtual Worlds: Societal, Technological, Economic and Policy Challenges for the EU*, 2023, https://publications.jrc.ec.europa.eu/ repository/handle/JRC133757.

account e aree riservate per accedere ai propri prodotti e servizi online. Nel metaverso, in particolare, questa esigenza diviene ancora più pressante, dato il maggior grado di esposizione dell'individuo, che arriva ad interagire sotto forma di avatar, e di condivisione dei suoi dati personali.

La creazione di un'identità digitale univoca e sicura si scontra con l'uso di soluzioni nazionali divergenti. Sul piano internazionale, il *Working Group IV* sul Commercio elettronico dell'Uncitral ha elaborato un *Model Law* per il reciproco riconoscimento delle identità e dei servizi fiduciari[79]. A livello europeo, proprio per affrontare adeguatamente le dinamiche dei mercati **e** gli sviluppi tecnologici, si è ritenuto necessario procedere all'aggiornamento e al perfezionamento del Regolamento eIDAS, in materia di identità e autenticazione digitali, pur mantenendone l'architettura di base. Il nuovo Regolamento eIDAS 2, infatti, specifica il diritto dei cittadini e dei residenti dell'Unione a un'identità digitale che sia sotto il loro controllo esclusivo e che consenta loro di esercitare i propri diritti nell'ambiente digitale e di partecipare all'economia digitale, per rendere effettivo il quale si esplicita la volontà di istituire un quadro armonizzato relativo all'identità digitale (v. cons. 5 e 6).

La *blockchain* è compatibile con questo disegno normativo. Sono state già citate[80], in questo senso, la Dichiarazione istitutiva della Blockchain Partnership Europea e la Risoluzione del Parlamento europeo del 3 ottobre 2018, che hanno posto in luce l'opportunità data dalla *blockchain* di superare i vecchi schemi incentrati sul controllo esterno delle identità in favore di un controllo diretto da parte degli interessati. Nel Report "*Blockchain and digital identity*" dello European Blockchain Observatory and Forum[81], la *blockchain* viene ritenuta un efficace strumento di sviluppo di identità digitali *self-sovereign*.

Il Regolamento eIDAS 2, non a caso, disciplina due nuovi strumenti che, pur non facendo diretto riferimento a una specifica tecnologia, potrebbero facilmente basarsi sulla tecnologia *blockchain*. Il primo è il registro elettronico, di cui si è detto *supra*[82]. Il secondo è il portafoglio europeo di identità digitale, definito come «un mezzo di identificazione elettronica che consente all'utente di conservare, gestire e convalidare in modo sicuro dati di identità personale e attestati elettronici di attributi al fine di fornirli alle parti facenti affidamento sulla certificazione e agli altri utenti dei portafogli europei di identità digitale, e di firmare mediante firme elettroniche qualificate o apporre sigilli mediante sigilli

[79] *Model Law on the Use and Cross-border Recognition on Identity Management and Trust Services*, https://uncitral.un.org/en/mlit.

[80] Vedi *supra,* par. 6.

[81] www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf.

[82] Vedi *supra*, par. 5.

elettronici qualificati» (art. 3, n. 42). La peculiarità del portafoglio europeo è la divulgazione selettiva dei dati personali da parte dell'utente e sotto il proprio esclusivo controllo (v. cons. 15).

La conformità delle soluzioni *blockchain-based* con il nuovo Regolamento eIDAS consentirebbero di realizzare gli obiettivi europei legati all'identità digitale. A riprova di ciò, la Commissione europea, nel delineare la propria Blockchain Strategy, ha riconosciuto il potenziale della *blockchain* di rivoluzionare il modo in cui si condividono le informazioni e si effettuano transazioni online, potendo migliorare il quadro europeo di identità digitale in evoluzione; conseguentemente, la Commissione ha inserito tra i "*gold standard*" per la *blockchain* l'identità digitale, che include la compatibilità della *blockchain* con le normative sulla firma elettronica, come eIDAS, e supporta un *framework* di identità ragionevole, pragmatico, decentralizzato e auto-sovrano.[83]

[83] https://digital-strategy.ec.europa.eu/it/policies/blockchain-strategy.