

## ***Blockchain e pubblica amministrazione: stato dell'arte e prospettive***

*Manfredi Matassa*

*La tecnologia blockchain sta catturando sempre più l'attenzione degli operatori del settore tecnologico e delle istituzioni italiane ed europee. Le molteplici applicazioni di questa tecnologia, in una prima fase accostate esclusivamente al settore finanziario, sembrano oggi avere una portata sterminata: servizi pubblici, tutela della privacy, identità digitale, tracciamento delle filiere produttive sono soltanto alcuni degli ambiti compatibili con quella che sembra poter essere una nuova rivoluzione industriale. Solo di recente, però, esse sono state oggetto di studio nell'ambito del diritto pubblico, aprendo nuovi orizzonti che non possono essere più esclusi dal dibattito della scienza dell'amministrazione. Il presente lavoro, oltre a fornire una panoramica sul dibattito inerente al delicato rapporto tra tecnologie emergenti e regolamentazione, intende mettere in luce i possibili ambiti di applicazione che la blockchain potrebbe trovare nell'ambito della pubblica amministrazione.*

### **1. Premessa**

La tecnologia *blockchain* sta catturando sempre più l'attenzione degli operatori del settore tecnologico e delle istituzioni italiane ed europee. Si ritiene che questa tecnologia, descritta come «macchina della verità» o, ancora, come «protocollo di Dio»<sup>1</sup>, stia per innescare una rivoluzione

<sup>1</sup> Entrambe le espressioni si leggono in M.J. CASEY, P. VIGNA, *La macchina della verità. La blockchain e il futuro di ogni cosa*, Milano, 2018. L'espressione "protocollo di Dio", un evidente richiamo all'opera del premio Nobel per la fisica Leon Lederman "The God Particle" che portò alla rivoluzionaria scoperta del bosone di Higgs, in realtà, ricorre già in N. SZABO, *The God Pro-*

digitale ancor più incisiva di quella avvenuta per mezzo dell'introduzione di internet nel 1993<sup>2</sup>.

Le molteplici potenzialità della tecnologia *blockchain* sono state già esplo-  
rate con riguardo ad alcuni profili specifici<sup>3</sup>. Solo di recente, però, esse  
sono state oggetto di studio nell'ambito del diritto pubblico<sup>4</sup>, aprendo  
nuovi orizzonti che non possono essere più esclusi dal dibattito della  
scienza dell'amministrazione.

*tocols*, 1999, reperibile su <https://nakamotoinstitute.org> (visitato il 10 ottobre 2021) per definire una tecnologia precorritrice della *blockchain*.

<sup>2</sup> Il possibile impatto della *blockchain* sulla società è stato paragonato a quello del *personal computer* negli anni Settanta e a quello di internet a metà degli anni Novanta. Già nel 2013 alcune compagnie statunitensi hanno sottolineato che la tecnologia *blockchain* avrebbe potuto raggiungere livelli di diffusione paragonabili a quelli di internet. Così A. WRIGHT, P. DE FILIPPI, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, 12 marzo 2015, 2-3, reperibile su SSRN: <https://ssrn.com/abstract=2580664> (visitato il 10 ottobre 2021). Altri come A. BORG, *Prefazione*, in A. BASILE, *Blockchain la nuova rivoluzione industriale*, Palermo, 2019, si sono spinti a sostenere «che è ormai una certezza che il fenomeno *blockchain* e criptovalute avrà un impatto simile, se non maggiore, a quello esercitato da *web* e *smartphone* in pochi anni». In senso opposto, invece, si veda K. LAW, E. MIK, *Pause the blockchain legal revolution*, in *British Institute of International and Comparative Law*, 69, 2020, p. 135 secondo cui «*the promised blockchain legal revolution appears to be a damp, and regrettably widely distributed, squib*».

<sup>3</sup> I primi studi hanno approfondito la *blockchain* in stretto legame con il *bitcoin* (e le criptovalute in generale). Tra questi si segnalano S. COPACCIOLI, *Criptovalute e Bitcoin: un'analisi giuridica*, Milano, 2015; D. CAPOTI, E. COLACCHI, M. MAGGIONI, *Bitcoin Revolution, la moneta digitale alla conquista del mondo*, Milano, 2015; N. VARDI, «*Criptovalute*» e dintorni: alcune considerazioni sulla natura giuridica dei *Bitcoin*, in *Dir. inform.*, 3, 2015, p. 443; G. GASPARRI, *Timidi tentativi giuridici di messa a fuoco del bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema*, in *Dir. inform.*, 3, 2015, p. 415.

<sup>4</sup> Per una panoramica generale sull'argomento può rinviarsi a G. GALLONE, *Blockchain, procedimenti amministrativi e prevenzione della corruzione*, in *Dir. ec.*, 3, 2019, p. 187 ss.; M. MACCHIA, *Blockchain e pubblica amministrazione*, in *Federalismi.it*, 2, 2021, p. 117; P. RUBECHINI, *Blockchain e pubblica amministrazione italiana: i primi passi di un cammino ancora lungo*, in *Giorn. dir. amm.*, 3, 2021, p. 298 ss.; S. CALDARELLI, *L'uso della tecnologia blockchain nel settore delle pubbliche amministrazioni: tra "mito" e realtà giuridica*, in *Dir. inform.*, 4, 2020, p. 857. Fra i contributi che hanno affrontato l'argomento con un taglio più specifico possono vedersi G. D'ACQUISTO, *Blockchain e GDPR: verso un approccio basato sul rischio*, in *Federalismi.it*, 2, 2021, p. 53 ss.; M. FARINA, *Blockchain e tutela della salute: verso la riorganizzazione dei sistemi sanitari?*, in *Federalismi.it*, 21, 2020, p. 170; M. VERZARO, *La blockchain e il fabbisogno di personale nella pubblica amministrazione*, in *Federalismi.it*, 2, 2021, p. 195 ss.; F. FAINI, *Il diritto nella tecnica: tecnologie emergenti e nuove forme di regolazione*, in *Federalismi.it*, 16, 2020, p. 79; G. GALLONE, *La pubblica amministrazione alla prova dell'automazione contrattuale. Note in tema di Smart Contracts*, in *Federalismi.it*, 20, p. 220, 142; G. GOMETZ, M. TAWA FOLARIN, *Voto elettronico presidiato e blockchain*, in *Ragion pratica*, 2, 2018, p. 317; M. MARCHESI, *Blockchain pubbliche e permissioned: una questione di fiducia*, in *Federalismi.it*, 2, 2021, p. 140 ss.

Sarebbe un errore, dunque, relegare l'approfondimento del tema dell'innovazione offerta dalla *blockchain* all'attenzione di informatici e appassionati. Infatti, ove questa tecnologia fosse (come sembra) realmente in grado di fornire una soluzione ad alcuni dei problemi più evidenti della pubblica amministrazione italiana, il ruolo attivo dello studioso del diritto amministrativo assumerebbe un'evidente rilevanza, anche perché l'elevato livello di complessità della tecnologia *blockchain* impone un coordinamento fra il mondo dell'informatica e quello del diritto<sup>5</sup>.

Sono trascorsi alcuni anni, ormai, da quando la dottrina più lungimirante ha cominciato ad avvertire che «*we stand at the edge of a new digital revolution*»<sup>6</sup>. Oggi la rivoluzione promessa è già in atto. La gara europea per la regolamentazione della *blockchain* è iniziata e vede in prima fila Stati come Malta, la Svizzera, Singapore, Gibilterra, Estonia, Svezia e Norvegia. L'Unione europea, tra le prime istituzioni a investire sugli sviluppi della nuova tecnologia<sup>7</sup>, ha creato già un osservatorio<sup>8</sup> e una *partnership* tra Stati con l'obiettivo di creare un'infrastruttura europea di servizi *blockchain*<sup>9</sup>.

<sup>5</sup> Ciò è essenziale per scongiurare una situazione simile a quella prospettata da K. LAW, E. MIK, *Pause the blockchain legal revolution*, cit., 136 in cui «*many lawyers do not understand the core technical terms in the blockchain narrative and incorrectly assume that they map directly onto similar legal terms. Concurrently, many technologists make false assumption about how legal rules work and thus imagine legal systems ripe for disruption*».

<sup>6</sup> Queste le parole iniziali del saggio di A. WRIGHT, P. DE FILIPPI, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, cit., p. 1.

<sup>7</sup> In un primo momento il fenomeno della *blockchain* è stato affrontato a livello unionale solo trasversalmente con la Risoluzione del Parlamento europeo del 26 maggio 2016 sulle valute virtuali, 2016/2007 INI, reperibile su [www.europarl.europa.eu](http://www.europarl.europa.eu). Tuttavia, dopo aver compreso le opportunità offerte dalla tecnologia a seguito dell'analisi approfondita compiuta dal Servizio Ricerca del Parlamento Europeo (ERPS), *Come la tecnologia blockchain può cambiarci la vita*, febbraio 2017, reperibile su [www.europarl.europa.eu](http://www.europarl.europa.eu), il legislatore europeo ha adottato la Risoluzione del Parlamento europeo del 3 ottobre 2018 sulle tecnologie di registro distribuito e *blockchain*: creare fiducia attraverso la disintermediazione, 2017/2772 (RSP) reperibile su [www.europarl.europa.eu](http://www.europarl.europa.eu).

<sup>8</sup> Il 1° febbraio 2018 la Commissione europea ha istituito *UE Blockchain Observatory & Forum* con l'obiettivo di consolidare la posizione dell'Europa come *leader* nello sviluppo di un ecosistema fondato su *blockchain*. L'osservatorio ha redatto numerosi report sui temi centrali che verranno affrontati durante la trattazione, per un maggior approfondimento si rinvia a [www.eublockchainforum.eu](http://www.eublockchainforum.eu) (visitato il 10 ottobre 2021).

<sup>9</sup> La *European Blockchain Partnership* (EBP) è un'iniziativa che ricomprende tutti gli Stati membri dell'UE e membri dello Spazio economico europeo (Norvegia e Lichtenstein) realizza-

Nell'aprire a un modello amministrativo di tale portata innovativa – vista anche (e soprattutto) l'occasione offerta dal piano del PNRR – l'Italia non solo avrebbe davanti a sé la possibilità di risolvere alcuni dei problemi strutturali della sua amministrazione, ma potrebbe approfittare della possibilità di compiere in un ruolo da protagonista un significativo passo su un percorso orientato verso il futuro.

## 2. Blockchain: *origine, funzionamento e caratteristiche*

L'origine della tecnologia *blockchain* è tradizionalmente riconnessa a un *paper* dal titolo *Bitcoin: A Peer-to-Peer Electronic Cash System*<sup>10</sup>, pubblicato sotto lo pseudonimo di Satoshi Nakamoto<sup>11</sup> il 31 ottobre 2008. Semplificando al massimo può dirsi che la *blockchain* nasce come registro digitale distribuito<sup>12</sup> a supporto del *bitcoin*. Questa tecnologia, tuttavia, dopo aver inizialmente catturato l'esclusiva attenzione degli operatori del mondo della finanza, da lì a qualche anno sarebbe stata considerata «il futuro di ogni cosa»<sup>13</sup>.

ta con l'obiettivo di valorizzare il potenziale dei servizi basati su *blockchain* a beneficio dei cittadini, della società e dell'economia. Come parte di questo impegno, tale partenariato fra Stati si sta impegnando a costruire un'infrastruttura europea di servizi *blockchain* (EBSI) con l'intento di fornire servizi pubblici transfrontalieri a livello dell'UE caratterizzati dai massimi livelli di sicurezza e *privacy*. Per un maggiore approfondimento del tema si rimanda a quanto può leggersi sul sito <https://ec.europa.eu>.

<sup>10</sup> S. NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, reperibile su <https://bitcoin.org/bitcoin.pdf> (visitato il 10 ottobre 2021).

<sup>11</sup> La reale identità di Satoshi Nakamoto, nonostante numerose speculazioni al riguardo, rimane a oggi sconosciuta. Per un maggiore approfondimento sulla questione si rimanda a A. O'HAGAN, *The Satoshi Affair*, in *London Review of Books*, XXXVIII, 13, 2016.

<sup>12</sup> La *blockchain* può definirsi come la forma più avanzata di registro distribuito (*Distributed Ledger Technology* o DLT) e si pone dunque come *species* all'interno del *genus* di questi ultimi. Per uno studio specifico sulla tecnologia DLT si rimanda a R. MAULL, P. GODSIF, C. MULLIGAN, A. BROWN, B. KEWELL, *Distributed ledger technology: Applications and implications*, in *Strategic Changes*, 26, 2017, p. 481. Più in generale, sul concetto di "centralizzazione" e "decentralizzazione" si rimanda a Y. BENKLER, *The Wealth of Networks: How Social Production Transforms Markets and Freedom*, New Haven, Yale University Press, 2006, p. 62 secondo cui «*centralization is a particular response to the problem of how to make the behavior of many individual agents cohere into an effective pattern or achieve an effective result. (...) Decentralization describes conditions under which the actions of many agents cohere and are effective despite the fact that they do not rely on reducing the number of people whose will counts to direct effective action*».

<sup>13</sup> Il riferimento è a M.J. CASEY, P. VIGNA, *La macchina della verità. La blockchain e il futuro di ogni cosa*, cit.

Individuare una definizione di *blockchain* non è un compito facile, in quanto non ne esiste una comunemente accettata né vi è un accordo sugli elementi minimi necessari per qualificare una tecnologia come tale<sup>14</sup>. Prima di procedere nel tentativo di spiegare il funzionamento, in ogni caso, sembra opportuno soffermarsi sulle circostanze che ne hanno determinato la creazione.

### 2.1 *L'origine della tecnologia: dal movimento Cypherpunk alle criptovalute*

La proposta di Nakamoto nasce nel solco di un'ideologia ben radicata. Già negli anni Ottanta del secolo scorso alcune delle menti più brillanti della matematica avevano avvertito l'esigenza di trovare un sistema che potesse permettere di raggiungere un consenso comune in assenza di un centro di raccolta delle informazioni<sup>15</sup>.

La necessità di trovare un sistema in grado di coordinare attività individuali senza un corpo centrale volto a proteggere i dati dalle possibili manipolazioni venne recepita da una rete di attivisti nota come movimento *Cypherpunk*. Tale movimento riteneva che solo una moneta elettronica anonima e funzionante su tecnologie crittografiche avrebbe permesso di realizzare sistemi di messaggistica sicuri, contratti digitali e sistemi di identità digitale rispettosi della *privacy*<sup>16</sup>.

Le ideologie poste alla base del movimento *Cypherpunk*, poi racchiuse da Eric Hughes nel «*Cypherpunk Manifesto*»<sup>17</sup>, presero vita nel 1994 con DigiCash, un sistema di pagamento virtuale creato dal matematico David Chaum per scambiare denaro in modo affidabile su internet in assenza di

<sup>14</sup> Per una riflessione più ampia sul corretto utilizzo del termine "*blockchain*" si rinvia a A. WALCH, *The Path of the Blockchain Lexicon (and the law)*, in *Review of Banking and Financial Law*, 36, 2016, p. 713.

<sup>15</sup> La questione, prima ancora dell'avvento di internet, era conosciuta in campo informatico come "il problema dei generali bizantini". Per un maggiore approfondimento si rinvia a L. LAMPERT, R. SHOSTAK, M. PEASE, *The Byzantine Generals Problem*, in *ACM Transactions on Programming Languages and Systems*, 4, 1982, p. 382.

<sup>16</sup> Per meglio comprendere il contesto culturale che a posto le basi per lo sviluppo del movimento *Cypherpunk* si veda P. VIGNA, M.J. CASEY, *The age of cryptocurrency: how Bitcoin and digital money are challenging the global economic order*, New York, 2015, p. 40.

<sup>17</sup> E. HUGHES, *A Cypherpunks Manifesto*, 9 marzo 1993, reperibile su <https://www.activism.net> (visitato il 10 ottobre 2021).

intermediari. Qualche anno dopo Nick Szabo, il collaboratore di Chaum che per primo offrì una definizione di *smart contract*<sup>18</sup>, pubblicò un breve scritto intitolato *The God Protocols*<sup>19</sup> nel quale sviluppava alcuni dei concetti basilari poi ripresi da Nakamoto. Quest'ultimo, poi, descrivendo il funzionamento di *bitcoin* nel 2008, riuscì a superare gli ostacoli che fino a quel momento avevano impedito il corretto funzionamento di un sistema di pagamento decentralizzato. Così, il 3 gennaio 2009, venne creato il blocco iniziale della *blockchain bitcoin* noto come *Genesis Block*<sup>20</sup>.

## 2.2 Cenni sul funzionamento della tecnologia

Lo sconosciuto inventore del *bitcoin*, coniugando in modo innovativo tecnologie da tempo esistenti in campo informatico, è riuscito a scongiurare il rischio del *double spending*<sup>21</sup> creando un registro visibile a tutti e al contempo immodificabile, capace di rendere superflua la presenza di intermediari per convalidare tutte le transazioni aventi per oggetto la moneta. Per comprendere il funzionamento della *blockchain* occorre dedicare alcuni cenni alle singole tecnologie di cui si compone<sup>22</sup>.

Anzitutto, la garanzia di integrità e paternità delle operazioni compiute all'interno del sistema sono garantite dall'utilizzo congiunto di due tecnologie: la cifratura a doppia chiave asimmetrica e le "impronte" di *hash*. Il primo, utilizzato in Italia per validare la firma digitale già dal 1997<sup>23</sup>, permette di assicurare l'origine, la paternità e l'immodificabilità

<sup>18</sup> N. SZABO, *Formalizing and Securing Relationships on Public Networks*, 1997, reperibile su <https://firstmonday.org/> (visitato il 10 ottobre 2021).

<sup>19</sup> N. SZABO, *The God Protocols*, cit.

<sup>20</sup> Sul punto si rimanda a U.W. CHOCHAN, *A History of Bitcoin*, 30 settembre 2017, 5, reperibile su SSRN: <https://ssrn.com/abstract/=3047875> (visitato il 10 ottobre 2021).

<sup>21</sup> Con l'espressione "*double spending*" si fa riferimento al rischio di ripetuto utilizzo della stessa risorsa da parte di un partecipante al *network*. Tale problema, sostanzialmente inesistente in un sistema a gestione centralizzata, nel quale è sufficiente tenere traccia di ogni transazione in uno o più *database* non modificabili dalla rete, sembrava non risolvibile in un sistema distribuito fino all'introduzione della tecnologia *blockchain*.

<sup>22</sup> Per una panoramica più approfondita delle varie tecnologie che compongono la *blockchain* si rimanda a F. SARZANA DI S. IPPOLITO, M. NICOTRA, *Diritto della blockchain, intelligenza artificiale e IoT*, Milano, 2018, p. 13 ss.

<sup>23</sup> La cifratura a doppia chiave asimmetrica, diffusa già nei primi anni Novanta del secolo scorso attraverso il *software Pretty Good Privacy* (PGP), è stata individuata dal legislatore italia-

di un messaggio attraverso il diverso utilizzo di una chiave di crittografia pubblica e una privata. L'impronta di *hash*<sup>24</sup> garantisce invece l'inalterabilità delle informazioni presenti nel registro permettendo di ricostruire in maniera cronologica la catena di blocchi<sup>25</sup>.

Un secondo elemento attiene alla struttura della *blockchain*, la quale è distribuita su un network *peer-to-peer* (P2P), in cui i singoli utenti operano come nodi del sistema agendo contemporaneamente da fruitori (*client*) e da distributori (*server*) delle informazioni immesse. Ciò, in sostanza, consente a ogni utente della rete di prendere visione e di prelevare i dati conservati nella memoria di massa di ciascun gruppo, rendendo così di fatto privo di utilità un attacco informatico a un singolo nodo.

In ultimo, è stato ripreso il principio della *proof of work*, già teorizzato nel 2004 da Hal Finney, come meccanismo di creazione del consenso<sup>26</sup> sia per validare le transazioni sia per incentivare gli utenti a mettere a

no quale tecnologia alla base della firma digitale già nel d.P.R. 10 novembre 1997, n. 513. Per una più attenta disamina dell'utilizzo della crittografia a doppia chiave asimmetrica si rimanda a A.G. OROFINO, *Forme elettroniche e procedimenti amministrativi*, Bari, 2008, p. 83 ss.

<sup>24</sup> Sul punto si richiama la puntuale definizione offerta da F. SARZANA DI S. IPPOLITO, M. NICOTRA, *Diritto della blockchain, intelligenza artificiale e IoT*, cit., p. 13: «la funzione di *hash* consente di ridurre in maniera univoca in insieme di *bit* in una stringa alfanumerica, univocamente riconducibile al contenuto originario, fornendo una sorta di "impronta digitale". Mentre non è possibile risalire al contenuto originario della stringa al risultato della funzione, eventuali modifiche di tale contenuto possono essere rilevate in quanto l'applicazione della funzione sul nuovo contenuto porterà la creazione di una stringa diversa».

<sup>25</sup> La questione dell'immutabilità delle transazioni è molto dibattuta fra gli addetti al settore poiché esiste pur sempre il rischio di un attacco inflitto attraverso il controllo della maggior parte dei nodi (fenomeno noto come "*Sybil attack*" o "*51% Attack*"). È bene fare presente che un simile attacco, oltre a essere di difficile attuazione, sarebbe di dubbia convenienza economica dal momento che costerebbe diversi miliardi di euro in termini di energia computazionale utilizzata. Sulla questione si rimanda a S. SAYEED, H.M. GHISBERT, *Assessing blockchain consensus and security mechanism against the 51% attack*, in *Applied Sciences*, 9, 2019, p. 1778, reperibile su <https://www.mdpi.com/2076-3417/9/9/1788> (visitato il 10 ottobre 2021). Bisogna inoltre sottolineare che, come chiarito da M.J. CASEY, P. VIGNA, *La macchina della verità. La blockchain e il futuro di ogni cosa*, cit., p. 53, qualsiasi tentativo di attacco al sistema attuato attraverso la sola brutta forza di calcolo apparirebbe del tutto inutile. Un chiaro esempio è offerto dalla *blockchain Bitcoin*: elaborare le combinazioni numeriche che potrebbero essere generate dall'algoritmo (SHA-256) posto a protezione dei dati contenuti nella rete con la rete computazionale più potente al mondo – cosa già di per sé impossibile, dato che al momento è la stessa rete *Bitcoin* – richiederebbe un periodo di tempo molto superiore all'età stimata del nostro universo.

<sup>26</sup> Per una panoramica più completa dei vari meccanismi di creazione del consenso in una rete distribuita si rimanda al catalogo offerto da F. SARZANA DI S. IPPOLITO, M. NICOTRA, *Diritto della blockchain, intelligenza artificiale e IoT*, cit., pp. 26-30.

disposizione risorse computazionali a beneficio della rete in modo da evitare possibili condotte fraudolente<sup>27</sup>.

Queste tecnologie sono state utilizzate per creare un *database* digitale distribuito che viene aggiornato, gestito, controllato e coordinato non a livello centrale, ma in modo decentralizzato, da parte di tutti coloro che vi accedono. La *blockchain*, come suggerisce il nome, altro non è che un registro organizzato in blocchi collegati in modo da formare una catena sequenziale marcata temporalmente. Ogni blocco contiene una serie di informazioni inserite dai nodi che hanno accesso alla *chain* e sono validate dalla maggioranza degli apparecchi collegati allo stesso *network*. Tutti questi dati, una volta immagazzinati nel relativo blocco, vengono cristallizzati in modo definitivo, per cui la loro modifica è possibile soltanto attraverso una operazione inversa sempre validata dalla maggioranza degli utenti. Ciò rende altamente improbabile, se non impossibile, la manipolazione dei dati e la modifica da parte di terzi non autorizzati.

La principale e potenziale caratteristica offerta da questa tecnologia, come di recente evidenziato in un rapporto del Ministero dello sviluppo economico (MISE), «è quella di ridurre, in alcuni casi anche drasticamente, il costo della fiducia necessario al perfezionamento di una transazione, intesa come scambio informativo o di valore, garantendo al tempo stesso certezza della sua esecuzione»<sup>28</sup>.

### 2.3 Tipologie di blockchain

Prima di confrontare le nozioni acquisite con il mondo del diritto pubblico si rende necessario fornire alcune nozioni di base sulle diverse

<sup>27</sup> Il meccanismo della *proof of work* richiede che determinati computer del *network* (generalmente identificati come “*miners*”) utilizzino la loro potenza computazionale per risolvere quesiti matematici e che gli altri, una volta risolto il quesito, verifichino che la soluzione non corrisponda a una transazione precedente. Per incentivare i *miners* a utilizzare la loro potenza computazionale a beneficio della rete è previsto un premio in criptovalute a beneficio dei nodi che hanno risolto il problema matematico. Per un maggiore approfondimento della questione si rimanda a J. BONNEAU, A. MILLER, J. CLARK, A. NARAYANAN, J. A. KROLL, E. W. FELTEN, *Research Perspectives and Challenges for Bitcoin and Cryptocurrencies*, in *IEEE Symposium on Security and Privacy*, 2015, 104 reperibile su <https://ieeexplore.ieee.org/document/7163021> (visitato il 10 ottobre 2021).

<sup>28</sup> MISE, *Proposte per la Strategia italiana in materia di tecnologie basate su registri conditi e Blockchain. Sintesi per la consultazione pubblica*, 2019, p. 3.

tipologie di *blockchain*<sup>29</sup>. Sebbene la questione verrà maggiormente approfondita nel prosieguo, occorre chiarire sin da subito che non tutte le tipologie possiedono le caratteristiche necessarie per poter dare un contributo significativo al raggiungimento degli obiettivi di efficienza e trasparenza che la pubblica amministrazione intende realizzare.

Le *blockchain* pure (*permissionless*) sono liberamente accessibili a chiunque voglia partecipare alla rete attraverso un meccanismo di consenso e sono prive di un'autorità centrale. Si tratta, cioè, di un modello sprovvisto di una figura proprietaria che non prevede alcuna barriera per l'accesso al *network*, ma anzi ne incentiva l'espansione tramite meccanismi di ricompensa per i suoi partecipanti.

Tali *blockchain* sono certamente idonee alla creazione di registri globali dall'elevato grado di affidabilità e sicurezza<sup>30</sup>, ma non sono compatibili con la stessa natura della pubblica amministrazione<sup>31</sup>, dal momento che nascono con lo specifico obiettivo di eliminare la necessaria presenza di soggetti istituzionali all'interno di un *network*<sup>32</sup>. Sebbene tale argomento possa considerarsi già sufficiente per escludere qualsiasi futura applicazione di questa tipologia di sistema, va ricordato che il funzionamento di una *blockchain permissionless* postula la presenza di un meccanismo di acquisizione del consenso che richiede in genere un non indifferente utilizzo di energia computazionale. In sistemi come *bitcoin* tale costo

<sup>29</sup> Un'analisi più precisa sulla questione è offerta da M. MARCHESI, *Blockchain pubbliche e permissioned: una questione di fiducia*, cit., p. 140 ss.

<sup>30</sup> Il sistema *permissioned*, oltre alla più celebre *blockchain Bitcoin*, è anche utilizzato in numerose *blockchain* progettate per la gestione degli *Smart Contracts* quali ad esempio *Ethereum*, *Waves*, *EOS*, *Qtum*, *Cardano*.

<sup>31</sup> Sulla compatibilità tra la natura della pubblica amministrazione e la *blockchain* si rimanda al contributo di S. CALDARELLI, *L'uso della tecnologia blockchain nel settore delle pubbliche amministrazioni: tra "mito" e realtà giuridica*, cit. p. 857 ss. in cui si è sottolineato come «l'applicazione dell'archetipo *blockchain* al settore pubblico porterebbe, di fatto, alla sostituzione della piattaforma alle amministrazioni intese come apparato (quindi nella loro dimensione soggettiva) e alle relative funzioni (stante l'inscindibile nesso tra organizzazione e attività amministrativa)».

<sup>32</sup> Per questa ragione i due opposti movimenti di stampo marxista e anarco-capitalista hanno visto nella tecnologia *blockchain permissionless* la possibilità di realizzare modelli di politiche pubbliche ispirati alla "governance senza governo". Per una puntuale ricostruzione sulla questione si rimanda a M. ATZORI, *Tecnologia blockchain e governance decentralizzata, lo Stato è ancora necessario?*, 1° dicembre 2015, reperibile su <http://ssrn.com/abstract=2709713> (vissuto il 10 ottobre 2021).

non costituisce un problema, poiché viene suddiviso tra i partecipanti (poi ricompensati con un premio in criptovalute), ma nel caso di una *blockchain* della pubblica amministrazione graverebbe sull'erario in assenza di qualsiasi strumento di compensazione.

Le tipologie di *blockchain* che sarebbero invece compatibili con il settore pubblico sono quelle di tipo privato (*permissioned*) o ibrido. Le prime non sono accessibili pubblicamente e prevedono che le autorizzazioni di scrittura e di lettura vengano gestite da uno o più soggetti selezionati (*master nodes*), mentre quelle ibride combinano le caratteristiche delle *blockchain permissionless* o *permissioned* a seconda delle esigenze. In passato l'utilizzo di tali tipologie è stato ritenuto poco efficiente e spesso posto in secondo piano rispetto ai sistemi tradizionali già disponibili, ma i dubbi sollevati appaiono facilmente risolvibili. La preoccupazione più fondata è riferita alla sicurezza del *network*, poiché l'assenza di meccanismi di validazione del consenso (*Proof of Work*, *Proof of Stake*, etc.) impone di affidare il sistema ad amministratori che potrebbero prendere il controllo dell'intera catena causando danni irreparabili.

Tale circostanza, tuttavia, non può considerarsi un ostacolo insuperabile. Alcuni studi, infatti, hanno individuato già misure specifiche in grado di risolvere il problema con assoluta sicurezza<sup>33</sup>. In quest'ottica l'utilizzo di *blockchain* private o ibride potrebbe garantire un grado di affidabilità e trasparenza sicuramente migliore rispetto a quello offerto dai sistemi tradizionali senza però comportare gli eccessivi costi richiesti dal funzionamento dei meccanismi di validazione del consenso.

Una volta chiarita l'affinità della *blockchain* con gli obiettivi di efficienza perseguiti dal settore pubblico, è possibile offrire una panoramica sugli ostacoli che sarà necessario superare per la sua regolazione.

<sup>33</sup> Si rimanda allo studio di M. MARCHESI, *Blockchain pubbliche e permissioned: una questione di fiducia*, cit., p. 148 che ha identificato una serie di specifiche caratteristiche che potrebbero conferire alle *blockchain* private gli stessi vantaggi delle *blockchain* pubbliche evitando al contempo i rischi di sicurezza del sistema (per esempio la presenza di un contratto chiaro per determinare obblighi e diritti dei partecipanti, tempi rapidi per la validazione delle transazione e utilizzo di un programma *explorer*).

### 3. *Il difficile equilibrio tra diritto e nuove tecnologie*

L'impatto economico e sociale della *blockchain* e delle altre tecnologie emergenti (IoT, IA, *big data*) ha imposto nuove riflessioni sul collegamento fra tecnologia e regolamentazione. Il legislatore, chiamato a individuare la migliore condotta di politica legislativa da mantenere di fronte a tali nuovi fenomeni, deve fare i conti con il fatto che queste tecnologie – o meglio le loro implicazioni nella società – si stiano evolvendo più velocemente della stessa legge (fenomeno noto in letteratura come *paceing problem*)<sup>34</sup>. La *governance* tecnologica, dunque, richiede un incisivo cambio di paradigma rispetto ai metodi di regolamentazione più tradizionali.

Anzitutto, seguendo la parabola della *lex informatica* come nuova *lex mercatoria*<sup>35</sup>, bisogna muovere dal presupposto che non tutte le tecnologie hanno bisogno di incontrare una specifica regolamentazione giuridica. Difatti, prima di avventurarsi nella codificazione di una determinata tecnologia innovativa, al legislatore spetta il compito di comprendere se l'eventuale assenza di regolamentazione potrebbe favorire il suo sviluppo, chiaramente senza ledere in alcun modo i diritti e le prerogative sociali. Solo qualora si giungesse a un esito negativo sarebbe poi opportuno

<sup>34</sup> Prima ancora dell'irrompere delle tecnologie oggetto di questa ricerca numerosi autori avevano evidenziato che l'innovazione tecnologica stava sempre più superando la capacità di leggi e regolamenti di stare al passo. Tra i principali contributi sul tema si vedano G. E. MARCHANT, B. R. ALLENBY, J. R. HERKERT, *The growing gap between emerging technologies and Legal-Etical Oversight*, Springer, 2011; L. DOWNES, *The laws of disruption: harnessing the new forces that govern life and business in the digital age*, New York, 2009; L.B. MOSES, *Recurring dilemmas: the law's race to keep up with technological change*, *University of Illinois Journal of Law, Technology & Policy*, 2007, p. 239; M. FENWICK, W.A. KAAL, E.P.-M. VERMEULEN, *Regulation Tomorrow: what happens when technology is faster than the law?*, *TILEC Discussion Paper*, 24, 2016, reperibile su <https://papers.ssrn.com/abstract=2834521> (visitato il 10 ottobre 2021), A. BUTENKO, P. LAROCHE, *Regulation for innovativeness or regulation of innovation?*, *TILEC Discussion Paper*, 7, 2015, reperibile su <http://ssrn.com/abstract=2584863> (visitato il 10 ottobre 2021). Tra i recenti contributi italiani, invece, si segnala F. FAINI, *Il diritto nella tecnica: tecnologie emergenti e nuove forme di regolazione*, in *Federalismi.it*, 16, 2020, p. 79.

<sup>35</sup> Si veda D.R. JOHNSON, D.G. POST, *Law and Borders: the Rise of Law in Cyberspace*, in *Stanford Law Review*, 1996, 1389 e F. MARRELLA, C.Y. YOO, *Is open source software the new lex mercatoria?*, in *Virginia Journal of International Law*, 4, 2007, p. 811. Inoltre, nel pionieristico contributo di A. WRIGHT, P. DE FILIPPI, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, cit., p. 1 ss., la *blockchain* (denominata "*lex Cryptographia*") è stata individuata come una nuova e più evoluta "*lex mercatoria*".

soffermarsi non soltanto sul “come”, ma anche sul “quando” e sul “che cosa” regolare<sup>36</sup>.

Per rispondere al primo interrogativo si è soliti procedere nel tentativo di ricondurre il fenomeno che si intende regolare in uno dei tre paradigmi (noti come “scatole”) di politica legislativa e di regolamentazione giuridica<sup>37</sup>. La prima categoria, quella della “scatola verde”, si applica nel caso in cui una nuova tecnologia non abbia alcun impatto sul sistema giuridico o sia riconducibile a una disciplina normativa già esistente (si pensi, ad esempio, al passaggio da una rete di comunicazione da tecnologia 4G o 5G). Nella seconda categoria, nota come “scatola nera”, rientrano quelle tecnologie il cui utilizzo potrebbe essere illegale e si richiede perciò una regolamentazione volta a vietarne l'utilizzo o a circoscriverlo a determinati usi e finalità. Il terzo paradigma è quello della *sandbox*, termine preso in prestito dal mondo informatico che indica un ambiente di prova controllato in cui i soggetti sono invitati ad agire in un contesto non regolamentato sotto la supervisione delle autorità competenti. In quest'ultima categoria sono racchiuse le tecnologie che potrebbero portare benefici alla comunità ma di cui non si conoscono i possibili effetti e implicazioni nel mondo del diritto<sup>38</sup>.

Se si applica quanto detto al tema della *blockchain* è possibile comprendere il delicato compito che il legislatore è chiamato a svolgere per la sua regolamentazione. La difficoltà principale sta nel fatto che le molteplici potenzialità di questa tecnologia non permettono di inquadrarla con precisione in uno dei contenitori descritti, sicché essa va ricondotta a paradigmi diversi a seconda del contesto in cui viene utilizzata. Per esempio, un registro interno di un'azienda funzionante su tecnologia

<sup>36</sup> Queste le riflessioni di M. FENWICK, W.A. KAAL, E P.-M. VERMEULEN, *Regulation Tomorrow: what happens when technology is faster than the law?*, cit., pp. 7-8.

<sup>37</sup> Per una più attenta disamina sulla questione si rinvia a J.A. MAUPIN, *Mapping the Global Legal Landscape of Blockchain and Other Distributed Ledger Technologies*, in *International Journal of Law and Information Technology*, 2017, p. 266 reperibile su <https://ssrn.com/abstract=2930077> (visitato il 10 ottobre 2021); F. SARZANA DI S. IPPOLITO, M. NICOTRA, *Diritto della blockchain, intelligenza artificiale e IoT*, cit., pp. 30-41.

<sup>38</sup> Sui tentativi di “*sandbox*” regolativa in materia di *blockchain* si rimanda a M. FENWICK, W.A. KAAL, E.P.-M. VERMEULEN, *Regulation Tomorrow: what happens when technology is faster than the law?*, cit., p. 25 ss.; F. SARZANA DI S. IPPOLITO, M. NICOTRA, *Diritto della blockchain, intelligenza artificiale e IoT*, cit., p. 34 ss.

*blockchain*, non generando impatti significativi a livello giuridico, potrebbe agevolmente essere inserito nel novero della “scatola verde”; per converso, un utilizzo delle criptovalute volto a eludere il fisco o all’acquisto di prodotti vietati nel c.d. *dark web* sarebbe da impedire e quindi da ricondurre alle “scatole nere”. In ambito finanziario, invece, la *blockchain* è stata approcciata globalmente attraverso il metodo della *sandbox*. Difatti, già nell’aprile del 2016 la UK *Financial Conduct Authority*, l’ente regolatore della finanza nel Regno Unito, ha avviato una *regulatory sandbox* con l’obiettivo di creare uno spazio sicuro in cui testare servizi finanziari utilizzando regole diverse da quelle stabilite dalle leggi in quel momento vigenti<sup>39</sup>. La possibilità di utilizzare *sandbox* regolatorie per facilitare lo sviluppo delle attività di tecno-finanza è stata di recente introdotta anche in Italia con l’art. 36, comma 2 *bis*, del d.l. 30 aprile 2019 n. 34 (c.d. decreto crescita)<sup>40</sup>.

Il caso che ha fatto comprendere però a tutto il mondo che la *blockchain* potrebbe avere implicazioni che la legislazione attuale non è in grado di affrontare è stato quello dell’attacco a un fondo di investimento, denominato *The DAO (The Decentralized Autonomous Organization)*, gestito interamente da un codice informatico<sup>41</sup>. Tale fondo intendeva realizzare un qualcosa di cui fino a quel momento si era discusso solo in teoria, cioè permettere ai sottoscrittori del fondo di votare le allocazioni degli investimenti proposte dall’algoritmo lasciando tuttavia la decisione circa

<sup>39</sup> UK FINANCIAL CONDUCT AUTHORITY, *Regulatory Sandbox*, 2015, reperibile su <https://fca.org.uk/publication/research/regulatory-sandbox.pdf> (visitato il 10 ottobre 2021).

<sup>40</sup> Art. 36, comma 2 *bis*, del decreto legge 30 aprile 2019, n. 34 convertito in legge 28 giugno 2019 n. 58: «Al fine promuovere e sostenere l’imprenditoria, di stimolare la competizione nel mercato e di assicurare la protezione adeguata dei consumatori, degli investitori e del mercato dei capitali, nonché di favorire il raccordo tra le istituzioni, le autorità e gli operatori del settore, il Ministro dell’economia e delle finanze, sentiti la Banca d’Italia, la Commissione nazionale per le società e la borsa (CONSOB) e l’Istituto per la vigilanza sulle assicurazioni (IVASS), adotta, entro centottanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto, uno o più regolamenti per definire le condizioni e le modalità di svolgimento di una sperimentazione relativa alle attività di tecno-finanza (FinTech) volte al perseguimento, mediante nuove tecnologie quali l’intelligenza artificiale e i registri distribuiti, dell’innovazione di servizi e di prodotti nei settori finanziario, creditizio, assicurativo e dei mercati regolamentati (...)».

<sup>41</sup> Per una panoramica completa sugli eventi che hanno coinvolto il progetto *The DAO* si rimanda a M.I. MEHAR, C.L. SHIER, A. GIAMBATTISTA, E. GONG, G. FLETCHER, R. SANAYHIE, H.M. KIM, M. LASKOWSKI, *Understanding a revolutionary and flawed grand experiment in blockchain: The DAO Attack*, in *Journal of Cases on Information Technology*, 1, 2019, p. 21.

l'utilizzo del capitale a quest'ultimo<sup>42</sup>. Si trattava, cioè, di un'applicazione estrema e letterale del noto concetto di Lawrence Lessig per cui «*the code is law*»<sup>43</sup> che intendeva porre rimedio all'inevitabile attitudine all'errore degli esseri umani attraverso un codice capace di individuare i più proficui investimenti. La scelta di sostituire con un algoritmo le più elementari garanzie generalmente necessarie per lo svolgimento in ambito finanziario (presenza di un capitale minimo a tutela degli investitori, requisiti di professionalità e onorabilità degli esponenti, trasparenza e obbligo di comunicazioni periodiche) sembrava però ignorare un'idea oggi perfettamente racchiusa nelle parole di Bruno Romano, e cioè che «la perfezione della macchina si inserisce nel mondo imperfetto degli uomini»<sup>44</sup>.

L'errore concettuale posto alla base di *The DAO* è divenuto evidente dopo soli pochi giorni dall'avvio della piattaforma, quando un sottoscrittore non identificabile riuscì a scrivere un programma capace di interagire con lo *smart contract* utilizzato dall'algoritmo per concludere le operazioni. In questo modo, attraverso centinaia di continue transazioni, vennero drenati dal fondo circa 55 milioni di dollari in appena un giorno (vi è infatti chi parla di «una versione virtuale di uno sportello bancomat fuori controllo»<sup>45</sup>). Ciò che rende questo evento un chiaro campanello d'allarme per la futura regolamentazione della tecnologia *blockchain* non è tanto l'avvenuto attacco, dovuto in realtà alle numerose vulnerabilità del codice evidenziate da alcuni esperti già al momento del suo lancio, ma il fatto che questo attacco informatico deve essere considerato perfettamente

<sup>42</sup> Pur essendosi ormai persa traccia della documentazione, i termini dell'accordo sono stati recuperati da M.J. CASEY, P. VIGNA, *La macchina della verità. La blockchain e il futuro di ogni cosa*, cit., p. 82: «il codice dello *Smart Contract* di *The DAO* governa la creazione dei *token* del fondo e prevale su qualsiasi affermazione relativa alla creazione di *The DAO* nel passato, nel presente o nel futuro».

<sup>43</sup> L. LESSIG, *Code and Other Law of Cyberspace*, New York, 1999. La base del concetto espresso da Lessig è stata sintetizzata nel recente contributo di F. LONGOBUCCO, *Smart contract e "contratto giusto": dalla soggettività giuridica delle macchine all'oggettivazione del fatto-contratto. Il ruolo dell'interprete*, in *Federalismi.it*, 2, 2021, p. 107: «il linguaggio robotico, incentrato sulla logica della aggregazione di dati e di fenomeni, aspira a generare la norma giuridica, intesa quale ordinamento del caso concreto».

<sup>44</sup> B. ROMANO, *Algoritmi al potere. Calcolo giudizio pensiero*, Torino, 2018, p. 59.

<sup>45</sup> M.J. CASEY, P. VIGNA, *La macchina della verità. La blockchain e il futuro di ogni cosa*, cit., p. 83.

legittimo. Il presunto *hacker* aveva trovato un modo per dialogare con la macchina nel rispetto del codice scritto dai fondatori di *The DAO* – e quindi, sulla falsariga del pensiero di Lessig, nel rispetto della stessa legge – lasciando così gli investitori del fondo sprovvisti di qualsiasi tutela. L'esempio appena riportato permette di rispondere con una certa sicurezza all'interrogativo sollevato circa la necessaria regolamentazione di questa nuova tecnologia in modo diametralmente opposto rispetto a quanto prospettato lo scorso ventennio da Lessig: il codice non può essere la legge. Per contro, la *blockchain* richiede precise scelte politico-legislative orientate a evitare lo scontro fra l'individuo, lo Stato e i mercati attraverso la ricerca del delicato punto di equilibrio tra gli interessi della sfera pubblica e gli interessi economici della sfera privata<sup>46</sup>. In altri termini, di fronte all'affermarsi di queste nuove tecnologie deve ritenersi quanto mai attuale il concetto espresso nel secolo passato dal filosofo Roscoe Pound secondo cui «*law must be stable, and yet it cannot stand still*»<sup>47</sup>.

### 3.1 *Quale disciplina per la blockchain?*

Come anticipato, per affrontare correttamente l'ambiziosa sfida della regolamentazione delle tecnologie emergenti non basta interrogarsi sul “che cosa”, ma anche sul “quando” e sul “come” disciplinare. Nel caso della *blockchain* le prime difficoltà che il legislatore è chiamato ad affrontare si presentano già nell'individuare con l'ambito dell'intervento regolatorio, ciò dal momento che ancora sono noti soltanto alcuni dei possibili ambiti applicativi che potranno coinvolgere questa rivoluzionaria tecnologia. Basti pensare che, se in una prima fase i dilemmi regolatori della *blockchain* riguardavano solo ed esclusivamente il settore finanziario, oggi le sue implicazioni sembrano avere una portata sterminata: servizi pubblici, tutela della *privacy*, identità digitale, sanità pubblica, tracciamento delle filiere produttive, rivoluzione energetica ed *e-voting* sono soltanto alcuni degli ambiti ritenuti compatibili con l'annunciata rivoluzione tecnologica.

<sup>46</sup> A. WRIGHT, P. DE FILIPPI, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, cit., p. 4.

<sup>47</sup> R. POUND, *Interpretations of Legal History*, New York, The Macmillan Company, 1923, p. 2.

Quanto al secondo interrogativo prospettato, quello del “quando”, va detto che neppure individuare il giusto momento per regolare può ritenersi un compito semplice per il legislatore. Quest’ultimo dovrà assicurarsi che la regolamentazione non sia adottata troppo presto, per evitare un disincentivo dello sviluppo tecnologico, ma neppure troppo tardi, per evitare i problemi derivanti dall’introduzione di una normativa acerba e inefficiente<sup>48</sup>.

L’ultimo profilo da tenere in considerazione riguarda il “come regolare” e va riferito alla forma e la sostanza della regolamentazione<sup>49</sup>. Nel caso della *blockchain*, esso coinvolge principalmente gli interrogativi relativi al livello di regolamentazione necessario per il raggiungimento degli obiettivi desiderati. Sul punto va evidenziato che, viste le già tratteggiate caratteristiche della tecnologia oggetto di questa ricerca, un approccio orientato allo sviluppo di una regolamentazione squisitamente nazionalistico non porterebbe con sé alcun risultato positivo. Basti pensare, per esempio, che l’unico effetto conseguente al tentativo dello Stato di New York di disciplinare i servizi basati su *blockchain* resi all’interno dello stato attraverso un *BitLicence Regulatory Framework* è stato quello di costringere la maggior parte degli operatori del settore a spostare la loro sede negli altri Stati privi di regolamentazione<sup>50</sup>. Risulta evidente, di conseguenza, che non potrà esistere una regolamentazione efficiente della *blockchain* che non sia il frutto di un’azione comune.

### 3.2 *L’assetto normativo vigente*

L’Unione europea, intuendo le innumerevoli potenzialità della tecnologia *blockchain*, è stata fra le prime istituzioni ad avventurarsi nella complessa sfida della regolamentazione di tale fenomeno attraverso la

<sup>48</sup> Per un maggiore approfondimento della questione si rinvia a G.E. MARCHANT, B.R. ALLENBY, J.R. HERKERT, *The growing gap between emerging technologies and Legal-Ethical Oversight*, cit., p. 23; L.B. MOSES, *Recurring dilemmas: the law’s race to keep up with technological change*, cit., p. 239.

<sup>49</sup> Sull’importanza del “*how regulate*” nel settore tecnologico si rimanda a R. BROWNSWORD, M. GOODWIN, *Law and technologies of the Twenty-First Century*, Cambridge, Cambridge University Press, 2012: *“In the law and technology stream, innovation is generally taken as an exogenous phenomenon, which occurs at a steady rate; the key issue is then how to regulate it.”*

<sup>50</sup> Sul tema si rimanda a P. YEOH, *Regulatory issues in blockchain technology*, in *Journal of Financial Regulation and Compliance*, 2, 2017, p. 196 ss.

già citata «Risoluzione del Parlamento europeo del 3 ottobre 2018 sulle tecnologie di registro distribuito e *blockchain*: creare fiducia attraverso la disintermediazione». Con tale risoluzione il Parlamento europeo, nell'evidenziare la sua intenzione di affermare l'Unione come *leader* del settore delle tecnologie DLT, ha invitato la Commissione a elaborare un quadro giuridico unitario in materia di tecnologie DLT incoraggiando al contempo gli Stati membri ad avviare una campagna di formazione, riqualificazione e sensibilizzazione in materia di competenze digitali. Nel fare ciò, sulla scorta di quanto già osservato nella richiamata analisi del 2017 dal titolo «come la tecnologia *blockchain* può cambiarci la vita», il legislatore europeo ha evidenziato la possibilità di applicare tale tecnologia in numerosi ambiti: tutela dell'ambiente, trasporti, settore sanitario, catene di approvvigionamento, istruzione, industrie creative e diritti d'autore, settore finanziario, infrastrutture pubbliche. È importante sottolineare che in questa prima fase di regolamentazione il legislatore europeo non ha preteso di trovare una disciplina già completa e funzionale di questa tecnologia emergente, ma si è limitato a individuare i principali ostacoli normativi capaci di limitarne lo sviluppo e la ricerca. Le tecnologie DLT, e quindi la *blockchain*, hanno trovato una specifica disciplina anche nella legislazione nazionale all'interno dell'art. 8-ter del d.l. 14 settembre 2018 n. 135, convertito in legge 11 febbraio 2019 n. 12, recante «disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione» (c.d. decreto semplificazione)<sup>51</sup>. Il primo comma di tale disposizione è stato inserito con l'intenzione di introdurre una definizione di DLT molto ampia e flessibile, adattabile a contesti sia pubblicistici sia privatistici, limitata a fungere come cornice giuridica per future linee guida la cui adozione è demandata all'Agenzia per l'Italia Digitale (AgID). Il contenuto dell'art.

<sup>51</sup> L'art. 8-ter, comma 1, del d.l. 14 settembre 2018 n. 135, rubricato «tecnologie basate su registri distribuiti e *smart contract*», ha inserito tali tecnologie in una cornice giuridica attraverso la seguente definizione: «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».

8-ter, comma 1, della c.d. legge semplificazione ha tuttavia sollevato diverse perplessità fra studiosi e operatori del settore.

Posto che la definizione proposta si sviluppa a partire da un'impresione di fondo riconducibile all'impropria sovrapposizione di concetti informatici diversi<sup>52</sup>, si riscontra molta incertezza in relazione alle caratteristiche utilizzate dal legislatore per qualificare un determinato *network* come *blockchain*. Più in particolare, nell'offrire la definizione di «registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturealmente decentralizzato su basi crittografiche, tali da consentire la registrazione la convalida, l'aggiornamento e l'archiviazione di dati (...) non alterabili e non modificabili», non si è tenuto in debita considerazione il problema dell'effettiva immutabilità delle informazioni contenute nella catena. Difatti, dal momento che nella remota ipotesi di "51% attack" (v. *supra*) un *network* funzionante sulla *PoW* potrebbe subire una modifica non voluta dei dati in esso contenuti, inserire nel linguaggio legislativo il concetto della non alterabilità delle informazioni per qualificare una determinata tecnologia di *blockchain* non si è rivelata la scelta più opportuna<sup>53</sup>.

L'art. 8-ter del d.l. 14 settembre 2018 n. 135 non si è limitato tuttavia a fornire una definizione di DLT, in quanto il terzo comma ha esteso alla memorizzazione di un documento informatico attraverso l'uso delle tecnologie basate su DLT gli effetti giuridici della validazione temporale elettronica (*timestamping*)<sup>54</sup>. Anche in questo caso la tecnica legislativa

<sup>52</sup> Come sottolineato da C. BOMPRESZI, *Commento in materia di Blockchain e Smart contract alla luce del nuovo Decreto Semplificazioni*, in *Dir. mer. tecn.*, 2019, p. 2 e da F. FAINI, *Il diritto nella tecnica: tecnologie emergenti e nuove forme di regolazione*, cit., p. 97 il legislatore sembra aver del tutto sovrapposto il concetto di "DLT" con quello di "*blockchain*", imprecisione che risulta ancor più evidente nel *dossier* informativo dei lavori parlamentari in cui si legge che «l'art. 8-ter, introdotto dal Senato, prevede la definizione normativa sia delle tecnologie basate su registri distribuiti (*blockchain*). Invece, come già chiarito *supra*, il rapporto tra tecnologie DLT e *blockchain* deve considerarsi di *genus a species*: la *blockchain* non è altro che un registro distribuito (DLT) che si avvale di particolari strumenti crittografici (cifratura a doppia chiave asimmetrica) e raggruppamento delle transazioni in blocchi regolati dalla funzione di *hash*. I due concetti, quindi, non sempre sono sovrapponibili.

<sup>53</sup> Sul concetto di immutabilità delle transazioni si rimanda a quanto evidenziato da A. WALCH, *The Path of the Blockchain Lexicon (and the Law)*, in *Review of Banking & Financial Law*, 36, 2017, p. 738 ss.

<sup>54</sup> Art. 8-ter, comma 3, d.l. 14 settembre 2018 n. 135: «la memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici

non può definirsi felice. Il generico rinvio all'art. 41 del regolamento (UE) n. 910/2014 non permette di chiarire a quale validazione temporale elettronica – qualificata o meno – il legislatore intenda fare riferimento<sup>55</sup>, poiché la norma richiamata regola gli effetti di entrambe le ipotesi di validazione. Si tratta di un interrogativo dal rilievo tutt'altro che teorico dal momento che solo sul *timestamping* qualificato vige in giudizio una presunzione di accuratezza circa la data e ora a cui la validazione fa riferimento, mentre in caso di validazione elettronica non qualificata la valutazione sarà rimessa al libero apprezzamento del giudice.

L'ulteriore previsione contenuta nel comma 4 dello stesso articolo, in cui viene affidato all'AgID il compito di individuare gli standard tecnici necessari per produrre gli effetti della validazione temporale qualificata, potrebbe suggerire che il legislatore intendesse riferirsi a entrambi i tipi di validazione<sup>56</sup>. Il documento contenente tali linee guida, tuttavia, non è stato ancora pubblicato, in quanto il gruppo di lavoro preposto ha ritenuto necessaria la previa risoluzione di questioni giuridiche ancora irrisolte<sup>57</sup>.

### 3.3 Blockchain e data protection: *una convivenza possibile?*

Un ulteriore nodo che il legislatore è chiamato a risolvere nella sfida della regolamentazione della tecnologia *blockchain* riguarda la sua compatibilità con la disciplina del regolamento europeo sulla protezione dei dati personali, meglio noto come GDPR (Reg. UE 2016/679)<sup>58</sup>. Prima di

ci della validazione temporale elettronica di cui all'art. 41 del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014».

<sup>55</sup> L'art. 41 del Regolamento eIDAS rubricato «effetti giuridici della validazione temporale elettronica» ha introdotto il principio di non discriminazione prevedendo che «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».

<sup>56</sup> C. BOMPRESZI, *Commento in materia di Blockchain e Smart contract alla luce del nuovo Decreto Semplificazioni*, cit., p. 2.

<sup>57</sup> Come sottolineato da A.M. GAMBINO, *Blockchain law: analisi tecnico-giuridica delle reti blockchain e degli smart contracts*, cit., p. 18, sarebbe stato più opportuno per il legislatore partire dal concetto di «elevata resistenza» del sistema ad attacchi esterni o manomissioni e non invece di «immutabilità».

<sup>58</sup> Il contenuto del regolamento è stato poi maggiormente adattato alla disciplina nazionale attraverso il d.l. 10 agosto 2018, n. 101, recante «disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del

approfondire tale questione, tuttavia, sembra opportuno fornire alcune nozioni di base sull'assetto normativo vigente in materia di *data protection*<sup>59</sup>.

Lo scopo principale del regolamento GDPR è quello di garantire «un elevato livello di protezione dei dati personali» in modo da porre rimedio alla frammentazione normativa prodotta dalla diversa attuazione nei vari Stati membri della precedente direttiva 95/46/CE. Per raggiungere tale obiettivo il legislatore europeo non solo ha introdotto regole orientate a una maggiore responsabilizzazione dei soggetti attivi del trattamento, ma ha anche ideato una serie di strumenti capaci di garantire agli interessati un uso più consapevole dei propri dati. Sul primo versante, le previsioni più incisive hanno riguardato sia l'individuazione obbligatoria di un soggetto titolare del trattamento dei dati, responsabile in forza del principio di *accountability*, sia un profondo mutamento della concezione del rischio di diffusione dei dati (non più valutato nel solo momento della violazione, ma anche in una fase preventiva e quindi potenziale). Sul secondo, invece, il GDPR ha dato maggiore risalto a esigenze di trasparenza nei confronti dell'interessato attraverso l'imposizione di un obbligo di informativa, seguita dall'ampliamento del diritto di accesso e la previsione di un diritto alla portabilità dei dati<sup>60</sup>.

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 e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)». Sul punto si veda G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d. lgs. 10 agosto 2018, n. 101*, Bologna, 2019.

<sup>59</sup> Sulla questione del rapporto tra *blockchain* e *data protection* si rimanda a M. BERBERICH, M. STEINER, *Blockchain Technology and the GDPR: How to Reconcile Privacy and Distributed Ledgers?*, in *European Data Protection Law Review*, 2, 2016, p. 422 ss.; L. MOEREL, *Blockchain & Data Protection ... and Why They are Not on a Collision Course*, in *European Review of Private Law*, 6, 2019, p. 825 ss.; A.M. GAMBINO, C. BOMPRESZI, *Blockchain e protezione dei dati personali*, in *Dir. inform.*, 3, 2019, p. 619 ss.; F. FAINI, *Blockchain e diritto: la «catena del valore» tra documenti informatici, smart contracts e data protection*, in *Resp. Civ. prev.*, 2, 2020, p. 297 ss.; G. D'ACQUISTO, *Blockchain e GDPR: verso un approccio basato sul rischio*, in *Federalismi.it*, 2, 2021, p. 53 ss.; M. BERBERICH, M. STEINER, *Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?*, in *Eur. Data Prot. L. Rev.*, 3, 2016, p. 422 ss.

<sup>60</sup> Per una panoramica generale delle misure adottate in concreto dal legislatore europeo per perseguire questi due obiettivi si rimanda a A.M. GAMBINO, C. BOMPRESZI, *Blockchain e protezione dei dati personali*, cit., 623.

Senza nulla aggiungere a quanto già messo in luce circa le innovazioni e le modifiche apportate alla normativa precedente è opportuno soffermarsi sulla definizione di “dati personali” offerta dall’art. 4 dello stesso GDPR, secondo cui per *personal data* si intende «qualsiasi informazione riguardante una persona fisica identificata o identificabile»<sup>61</sup>. Si tratta di un punto per nulla estraneo al tema della *blockchain* se si considera che tale definizione potrebbe ritenersi sufficientemente ampia da ricomprendere anche le chiavi asimmetriche poste alla base dei suoi meccanismi crittografici. Difatti, dal momento che è pur sempre sufficiente conoscere la chiave privata di decodifica per riportare il dato alla sua forma intellegibile direttamente identificativa, le informazioni protette da tale tipologia di cifratura sono da considerare indirettamente identificabili<sup>62</sup>. Allo stato dell’arte, pertanto, la soluzione più corretta sembra quella orientata ad attrarre i dati contenuti in *network* funzionanti su *blockchain* alle prescrizioni del GDPR in quanto anonimi e non pseudonimi<sup>63</sup>. Tuttavia, sebbene tale tecnologia potrebbe assicurare una gestione trasparente

<sup>61</sup> I dati personali sono definiti dall’art. 4 dello stesso GDPR come «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».

<sup>62</sup> Sul tema si veda G. D’ACQUISTO, *Blockchain e GDPR: verso un approccio basato sul rischio*, cit., p. 57, il quale ha chiarito che «in un dato composto (...) qualsiasi elemento, intellegibile o meno, è idoneo a identificare un interessato. Basta infatti che quell’elemento sia noto a un terzo e riconosciuto da questi come un attributo di una specifica persona (si parla di informazione ausiliaria disponibile a un terzo) per creare un collegamento tra l’identità e il dato, che è ciò che chiamiamo intellegibilità». In senso opposto, invece, si veda F. RAMPONE, *I dati personali in ambiente blockchain tra anonimato e pseudonimato*, in *Cyberspazio e Diritto*, 3, 2018, p. 457 ss. il quale ha concluso che «[p]rogettare un protocollo *blockchain* (pubblico o privato che sia) in modo tale che le soluzioni crittografiche impiegate non debbano considerarsi dati pseudonimi, è possibile, ed è anche la regola, sicché la *blockchain*, anziché rappresentare un rischio per i diritti e la libertà fondamentali dell’individuo in termini di *privacy*, sarà lo strumento che metterà definitivamente nelle mani dei soggetti interessati la disponibilità esclusiva e il controllo dei loro dati».

<sup>63</sup> La pseudonimizzazione è stata definita dall’art. 4 del GDPR come: «il trattamento dei dati personali in modo tale che i possano più essere attribuiti a un interessato specifico senza l’utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile». Quanto alla *blockchain*, in cui l’identità di qualsiasi componente della rete può essere nota ai possessori della chiave sua privata, il Parlamento europeo nella già citata risoluzione del 3 ottobre 2018

delle informazioni e una maggiore resistenza ad attacchi informatici diretti alla loro violazione, non può nascondersi un certo attrito fra le principali caratteristiche di tale tecnologia il rinnovato quadro regolamentare europeo in materia di *privacy*.

Senza alcuna pretesa di esaustività, è possibile porre in evidenza alcuni aspetti di frizione della tecnologia in esame con alcuni dei principi generali enucleati dal reg. UE 2016/679<sup>64</sup>.

Anzitutto, non sembra facile la convivenza tra le modalità di distribuzione delle informazioni su rete *blockchain* e il principio di minimizzazione dei dati sancito dall'art. 5, comma 1, lett. c) del GDPR, secondo cui devono essere elaborati solo i dati adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati, intendendosi per minimizzazione «una riduzione al minimo del numero dei dati, del tipo dei trattamenti, dei soggetti che a vario titolo possono avere contezza dei dati, del periodo di conservazione»<sup>65</sup>. Appare infatti evidente che un'infrastruttura in cui le informazioni inserite fungono da base su cui aggiungere le nuove informazioni e sono accessibili a tutti i nodi della catena potrebbe essere ontologicamente incompatibile con le finalità perseguite da tale principio. La conservazione perpetua dei dati in *blockchain* confligge altresì con il principio di limitazione della conservazione dei dati statuito dall'art. 5, comma 1, lettera e), del GDPR, secondo cui «i dati personali devono essere conservati fino a quando sono per finalità per le quali vengono raccolti, ammettendosi una conservazione nel pubblico interesse, di ricerca scientifica o storica o per fini statistici».

L'ostacolo normativo che appare più difficilmente superabile sembra tuttavia quello del diritto alla cancellazione dei dati – noto anche come “diritto all'oblio” – disciplinato dall'art. 17 del regolamento 679/2016<sup>66</sup>.

ha chiarito che le tecnologie DLT promuovono «la pseudonimizzazione degli utenti, ma non la loro anonimizzazione».

<sup>64</sup> Per una più attenta disamina sui singoli profili di contrasto tra la tecnologia *blockchain* e il regolamento GDPR si rimanda a A.M. GAMBINO, C. BOMPRESZI, *Blockchain e protezione dei dati personali*, cit., p. 619 ss.

<sup>65</sup> N. BERNARDI (a cura di), *Privacy: protezione e trattamento dei dati*, Milano, 2020, p. 82.

<sup>66</sup> Prima di trovare una compiuta disciplina all'interno dell'art. 17 del reg. UE 2016/679 il diritto all'oblio si è affermato nel nostro ordinamento (sebbene con una dimensione più tradizionale indirizzata alla tutela della riservatezza) ancor prima dell'avvento di internet grazie all'ap-

Oltre a un punto di frizione piuttosto evidente, e cioè che l'utilizzo di una piattaforma ideata per garantire la tracciabilità di tutte le transazioni mal si concilia con un diritto introdotto per soddisfare «il comprensibile desiderio e l'aspirazione dell'uomo a essere dimenticato»<sup>67</sup>, emergono dei problemi ricollegati al fatto che tale diritto può essere esercitato solamente dopo la previa individuazione del titolare del trattamento dei dati personali<sup>68</sup>. Compito, quest'ultimo, non affatto agevole in un'infrastruttura *blockchain*<sup>69</sup>.

Dall'analisi fin qui svolta potrebbe desumersi che la tensione tra il GDPR e la natura stessa della *blockchain* costituisca un blocco insuperabile per lo sviluppo di questa nuova tecnologia. Tuttavia, l'Osservatorio Blockchain dell'Unione europea ha analizzato la questione in uno specifico report giungendo a una soluzione diametralmente opposta, e cioè che «*there is no contradiction in principle between the goals of the GDPR and those of blockchain technology*»<sup>70</sup>. Più precisamente, dopo aver riconosciuto l'esistenza di un problema di compatibilità tra la

porto della dottrina più avveduta. Tra i primi contributi sull'argomento si veda T.A. AULETTA, *Diritto alla riservatezza e "droit a l'oubli"*, in G. ALPA (a cura di), *L'informazione e i diritti della persona*, Napoli, 1983, p. 127 ss.; G.B. FERRI, *Diritto all'informazione e diritto all'oblio*, in *Riv. dir. civ.*, 1990, p. 801 ss.; G. GIACOBBE, *Diritto all'oblio*, in E. GABRIELLI (a cura di), *Atti del convegno di Urbino 17 maggio 1997*, Napoli, 1999, p. 30 ss.; M.R. MORELLI, voce *Oblio (diritto all')*, in *Enc. dir.*, VI, Milano, 2002, p. 851 ss.

<sup>67</sup> M. TAMPERI, *Il diritto all'oblio e la tutela dei dati personali*, in *Resp. Civ e prev.*, 3, 2017, p. 1015.

<sup>68</sup> La definizione di «titolare del trattamento» è offerta dall'art. 4, punto 7), del GDPR come «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o dagli Stati membri».

<sup>69</sup> L'individuazione del titolare del trattamento si presta a difficoltà a causa del carattere distribuito, decentralizzato della *blockchain* nonché della condizione di pseudonimato dei partecipanti della catena. Una possibile soluzione alla questione è stata tuttavia prospettata da G. D'ACQUISTO, *Blockchain e GDPR: verso un approccio basato sul rischio*, cit., pp. 56-37, il quale ha suggerito di identificare il titolare del trattamento nei nodi capaci di determinare le finalità e le modalità di trattamento dei dati personali (ove presenti) o, in assenza di nodi qualificati, nel soggetto che decide di utilizzare la *blockchain*.

<sup>70</sup> Il riferimento è al *report* tematico pubblicato il 28 ottobre 2018 dall'*UE Blockchain Observatory & Forum* della Commissione europea dal titolo «*Blockchain and the GDPR*», 17-18, reperibile su [www.eublockchainforum.eu](http://www.eublockchainforum.eu) (visitato il 10 ottobre 2021).

*blockchain* e la normativa europea in materia di *privacy*, l'Osservatorio istituito dalla Commissione ha ritenuto sufficienti alcuni chiarimenti dei soggetti regolatori – su tutti l'*European Data Protection Board* (EPDB) – in relazione ai temi oggetto dei diversi punti di frizione. Tra questi il *report* ha suggerito alle autorità competenti di identificare con maggiore precisione le corrette modalità di identificazione e di utilizzo dei dati personali nonché di prendere una posizione ancor più netta sulla questione dell'effettiva anonimizzazione degli stessi. Attesa l'importanza strategica offerta dai possibili sviluppi di questa tecnologia, è comunque auspicabile un intervento del legislatore sovranazionale volto a inserire una disciplina unitaria della *blockchain* priva di conflitti con le altre norme fondamentali dell'Unione.

Il quadro normativo appena descritto non rappresenta altro che un primo timido passo diretto ad esplorare la possibilità di raggiungere l'obiettivo di una disciplina della tecnologia *blockchain* capace di sviluppare a pieno il suo potenziale. Prestando particolare attenzione alle implicazioni di questa tecnologia nella sfera pubblica, va detto che la rivoluzione promessa *blockchain* non potrà prendere forma in assenza di una disciplina specifica dedicata ai diversi ed eterogenei settori interessati della pubblica amministrazione.

#### **4. I possibili utilizzi della blockchain nella pubblica amministrazione**

Il settore della pubblica amministrazione è stato uno dei primi a essere chiamato a occuparsi del rapporto fra diritto e innovazione tecnologica. Il dibattito su processo di informatizzazione della pubblica amministrazione ha catturato gli interessi degli studiosi del diritto pubblico ancora prima della creazione di internet<sup>71</sup> e sembra aver assunto una nuova centralità. Inizialmente il concetto di "informatizzazione" è stato sovrapposto a quello di "digitalizzazione", il cui obiettivo era quello di

<sup>71</sup> Per uno studio sulla ricostruzione delle tappe della digitalizzazione e dei suoi più recenti sviluppi si rimanda a P. GIACALONE, *La normativa sul governo elettronico*, Milano, 2007; A.G. OROFINO, *Forme elettroniche e procedimenti amministrativi*, Bari, 2008, p. 193 ss.; B. SELLERI, *Gli atti amministrativi in forma elettronica*, in *Dir. soc.*, 1982, p. 141; E. CARLONI, *Tendenze recenti e nuovi principi della digitalizzazione pubblica*, in *Giorn. Dir. Amm.*, 2, 2015, p. 148 ss.; F. CARDARELLI, *Amministrazione digitale, trasparenza e principio di legalità*, in *Dir. inf.*, 2, 2015, p. 227 ss.; e M.L. MADDALENA, *La digitalizzazione della vita dell'amministrazione e del processo*, in *Foro amm.*, 10, 2016, p. 2535 ss.

organizzare l'apparato pubblico in modo da abbandonare il cartaceo in favore della forma elettronica. In questa prima fase, l'informatizzazione della pubblica amministrazione è stata da molti considerata alla stregua di un fenomeno endogeno utile a soli scopi organizzativi e quindi «incapace di condizionare la sostanza del procedimento»<sup>72</sup>. A partire dagli anni Ottanta del secolo scorso, però, sono incominciate a emergere in dottrina alcune lungimiranti voci che non hanno mancato di sottolineare la capacità di questo processo di incidere profondamente sulla sostanza dell'amministrazione e, per l'effetto, sulla vita del cittadino<sup>73</sup>. A oggi, vista l'enorme potenzialità offerta dalle tecnologie emergenti, pare chiaro che gli obiettivi dell'informatizzazione non debbano essere più limitati alla mera semplificazione dell'attività amministrativa, ma a una sua radicale ridefinizione<sup>74</sup>. La *blockchain* rientra fra le tecnologie che potrebbero avere un impatto significativo sul modello tradizionale di amministrazione, ma occorre procedere con le dovute cautele. Poiché si tratta di tecnologie in fase di rapida evoluzione e dagli effetti ancora non del tutto noti, prima di procedere con lo sviluppo dei casi d'uso sarà necessario maturare sufficienti elementi di valutazione delle diverse opzioni disponibili nel paradigma di adozione. Ciò, come suggerito dal MISE, «dovrà farsi con un approccio olistico che consideri attentamente gli obiettivi specifici dei vari contesti applicativi, ovvero i requisiti tecnico-giuridici da soddisfare e le possibili implicazioni di natura etica e sociale, anche di lungo periodo»<sup>75</sup>.

Prima di inquadrare i possibili utilizzi di tale tecnologia nell'attività amministrativa e in alcuni settori dell'organizzazione è tuttavia opportuno

<sup>72</sup> In questi termini G. GALLONE, *Blockchain, procedimenti amministrativi e prevenzione della corruzione*, cit., p. 187.

<sup>73</sup> Il riferimento è a G. DUNI, *L'utilizzabilità delle tecniche elettroniche nell'emanazione degli atti e nei procedimenti amministrativi. Spunto per una teoria dell'atto amministrativo emanato in forma elettronica*, in *Riv. Amm. R.I.*, 1978, p. 407 ss.; A. USAI, *Le prospettive di automazione delle decisioni amministrative in un sistema di teleamministrazione*, in *Dir. inf.*, 1993, p. 164 ss.; A. SCALA, *L'automazione nella redazione degli atti amministrativi*, in *Nuova rass.*, 1995, p. 1792 ss.

<sup>74</sup> B. CAROTTI, *L'amministrazione digitale: le sfide culturali e politiche del nuovo Codice*, in *Giorn. dir. amm.*, 2017, 1, p. 15.

<sup>75</sup> MISE, *Proposte per la strategia italiana in materia di tecnologie basate su registri condivisi e blockchain*, cit., 20.

segnalare le differenze tra due alternativi modelli teorici di *blockchain governance*<sup>76</sup>.

Il primo, noto come *blockchain administration*, intende utilizzare la tecnologia in commento per permettere ai cittadini di operare in condizione di parità per soddisfare i loro interessi attraverso un sistema *peer to peer* e non invece rapportandosi con un'autorità centrale dotata di potere amministrativo. Il secondo, noto come *blockchain for public administrations*, vuole invece allontanarsi dalla forma più pura della tecnologia (quella *permissionless*) in modo da plasmarla all'assetto ordinamentale volto a regolare il rapporto giuridico tra pubblici poteri e cittadini.

Va chiarito subito che l'idea di utilizzare una *blockchain permissionless* per realizzare un modello estremo di *open government*<sup>77</sup> è impraticabile tanto per ragioni di tenuta generale dell'assetto vigente quanto per ragioni squisitamente pratiche. Anzitutto, non bisogna dimenticare che la *blockchain* è pur sempre una tecnologia sviluppata con lo specifico obiettivo di permettere lo svolgimento di transazioni in sistemi complessi senza la necessaria presenza di un apparato centrale dotato della fiducia dei partecipanti. L'operazione di decentralizzazione conseguente all'ipotetico utilizzo di una forma "pura" di questa tecnologia nel settore pubblico non si limiterebbe dunque a ridimensionare il ruolo della pubblica amministrazione – istituzione "di fiducia" per eccellenza – all'interno dello Stato, ma la renderebbe del tutto superflua.

Il punto non è dunque comprendere se, in un simile scenario cripto-anarchico, la *blockchain administration* potrebbe garantire una maggiore efficienza della macchina amministrativa, ma stabilire se in tale ipotesi esisterebbe ancora una pubblica amministrazione. Quest'ultima, infatti, anziché curare gli interessi pubblici individuati dalla legge, trarrebbe la sua legittimazione all'esercizio del potere direttamente dai meccanismi di consenso previsti dalla piattaforma. Così, esonerando lo Stato dal

<sup>76</sup> Un'analisi della questione è offerta da S. CALDARELLI, *L'uso della tecnologia blockchain nel settore delle pubbliche amministrazioni: tra "mito" e realtà giuridica*, cit., p. 865 ss.

<sup>77</sup> Per un approfondimento di ampio respiro sul concetto di *open government* si rimanda a E. CARLONI, *L'amministrazione aperta. Regole strumenti limiti dell'open government*, Rimini, 2014; E. DI BLASIO, *Il governo online: nuove frontiere della politica*, Roma, 2018. Un'analisi delle iniziative più rilevanti è invece offerta da R. DE ROSA, V. REDA, *Open Government: disegnare la partecipazione per la società del futuro*, in *Comunicazione politica*, 3, 2017, p. 537 ss.

compito di gestire funzioni e servizi pubblici, si creerebbe un inaccettabile sistema distopico di “amministrazione dei cittadini per i cittadini” del tutto estraneo al controllo dell’apparato pubblico.

Oltre a ciò, non può omettersi di considerare un’altra ragione che si frappone all’idea di realizzare un modello di *governance* basato su un’infrastruttura *blockchain* pubblica, e cioè la vocazione transnazionale della tecnologia. Infatti, dal momento che l’archetipo originario della tecnologia ideata da Nakamoto non permette di individuare *ex ante* i partecipanti alla piattaforma, sarebbe impossibile circoscrivere l’accesso alla piattaforma ai confini di un determinato territorio. Peraltro, anche qualora si intendesse superare quest’ostacolo attraverso la creazione di una struttura *blockchain* ibrida ma fedele agli stessi scopi, gli elevati costi ricollegati ai meccanismi del consenso che sarebbero riversati sui cittadini (su tutti la *Proof of Work*) renderebbero quantomeno dubbia l’economicità di tale misura.

A parer di chi scrive, sarà possibile ideare un modello di *blockchain governance* solo allontanandosi dalla versione più pura della tecnologia in commento. L’unico modello in astratto perseguibile è infatti da considerare quello della *blockchain for public administrations*, il quale vede un impiego della *blockchain* a servizio, e non in sostituzione, dell’apparato amministrativo. Solo partendo da tale presupposto sarà possibile inquadrare i possibili utilizzi di tale tecnologia nell’attività amministrativa e in alcuni settori dell’organizzazione.

#### 4.1 Blockchain, *procedimenti amministrativi e i limiti delle decisioni automatizzate*

Come anticipato, la parziale decentralizzazione garantita dalle piattaforme *blockchain permissioned* o ibride, potrebbe contribuire alla formazione di un procedimento amministrativo più trasparente ed efficiente sul piano della gestione dei costi. Si tratta, tuttavia, di un tema estremamente delicato, in quanto l’inevitabile spinta centrifuga conseguente all’utilizzo di tale sistema è in grado di mutare radicalmente la fisionomia del procedimento amministrativo. Un suo accurato utilizzo nell’attività amministrativa permetterebbe di dare un nuovo significato alla partecipazione del privato nella formulazione delle decisioni amministrative: i cittadini potrebbero abbandonare il ruolo di destinatari dell’attività amministra-

tiva per assumere un ruolo inedito all'interno del procedimento, ossia quello di co-titolari della funzione con la stessa amministrazione<sup>78</sup>. Ciò, chiaramente, dovrebbe essere attuato tenendo ben presente che la presenza della macchina potrà al massimo ridimensionare, e non invece rendere del tutto superflua, la necessità di un attore pubblico titolare di un potere autoritativo<sup>79</sup>.

Inoltre, anche qualora si optasse per lasciare inalterata l'attuale struttura del procedimento, è indubbio che la creazione di un sistema basato su *blockchain* porterebbe con sé diversi benefici nell'ambito della trasparenza amministrativa. La tecnologia in esame permetterebbe infatti di inserire tutte le informazioni relative a una decisione assunta con gli strumenti tradizionali in un registro decentralizzato, e al contempo immutabile, messo direttamente a disposizione dei cittadini o di gruppi più ristretti di interessati, rendendo così superflua l'intera disciplina dell'accesso agli atti così come oggi conosciuta (documentale, civico e generalizzato).

Con riferimento ad ambiti più specifici, può ritenersi che la *blockchain* potrebbe migliorare sensibilmente il settore dell'evidenza pubblica tanto nella fase procedimentale quanto in quella negoziale. Nella fase della scelta del contraente i vantaggi offerti dalle caratteristiche della *blockchain* si dimostrano piuttosto evidenti. Un registro visibile a tutti e al contempo immodificabile permetterebbe di garantire con assoluta certezza l'integrità delle offerte presentate dai partecipanti, evitando al contempo qualunque tipo di interferenza illecita da parte degli attori pubblici. In un simile scenario, tutti i partecipanti alla procedura potrebbero verificare la data e l'ora della presentazione delle offerte e, una volta scaduti i termini per la loro presentazione, anche il loro contenuto. Dunque, nella fase iniziale delle gare un eventuale utilizzo della *blockchain* non solo non incontrerebbe particolari problemi applicativi ma sembrerebbe poter contribuire alla creazione di un procedimento più efficiente e trasparente.

<sup>78</sup> In questi termini G. GALLONE, *Blockchain, procedimenti amministrativi e prevenzione della corruzione*, cit., p. 202.

<sup>79</sup> Si riporta, tra le tante, la posizione di M. MACCHIA, *Blockchain e pubblica amministrazione*, cit., p. 127 secondo cui la *blockchain* «può essere impiegata come supporto ma non può essere sostitutiva del responsabile amministrativo».

La questione, tuttavia, diventa ben più complessa nel momento in cui si intende utilizzare la macchina per determinare la scelta del contraente<sup>80</sup>. Sebbene il principio del divieto di decisioni “esclusivamente” automatizzate originariamente enucleato dalla giurisprudenza amministrativa di primo grado<sup>81</sup> possa ritenersi stemperato dal più permissivo orientamento del Consiglio di Stato<sup>82</sup>, non può ignorarsi quanto affermato sul punto dall’art. 22 del regolamento (UE) 679/2016. La citata disposizione, dopo aver affermato il diritto del cittadino a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, permette di derogare tale diritto alla sola presenza di tre condizioni predeterminate: se necessario per la conclusione o l’esecuzione di un contratto fra l’interessato e un titolare del trattamento; se autorizzato dal diritto dell’Unione europea o dello Stato membro cui è soggetto il titolare del trattamento; se vi è consenso esplicito dell’interessato. Per operare nel pieno rispetto dei canoni europei, dunque, le potenzialità offerte dalla gestione algoritmica della fase pubblicistica delle procedure a evidenza pubblica dovrebbero incontrare una più attenta analisi del legislatore. Come preannunciato, però, i possibili utilizzi della *blockchain* nell’ambito dell’evidenza pubblica non si esauriscono nella fase di scelta del contraente, ma vanno estesi anche (e forse soprattutto) alla fase privatistica successiva all’aggiudicazione<sup>83</sup>. Si tratta di un punto di grande interesse

<sup>80</sup> Tra la sterminata letteratura che ha approfondito il rapporto tra algoritmi e pubblica amministrazione si rimanda a A. PAJNO, M. BASSINI, G. DE GREGORIO, M. MACCHIA, F.P. PATTI, O. POLLICINO, S. QUATTROCOLO, D. SIMEOLI, P. SIRENA, *Al: Profili giuridici. Intelligenza artificiale: criticità emergenti e sfide per il giurista*, in *Biola Journal*, 3, 2019; A. SIMONCINI, *Profili costituzionali della amministrazione algoritmica*, in *Riv. trim. dir. pubbl.*, 4, 2019, p. 1149 ss.; B. CAROTTI, *Algoritmi e poteri pubblici: un rapporto incendiario*, in *Giorn. dir. amm.*, 1, 2020, 5 ss.; S. CRISCI, *Intelligenza artificiale ed etica dell’algoritmo*, in *Foro amm.*, 10, 2018, p. 1787; L. VIOLA, *L’intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell’arte*, in *Foro amm.*, 9, 2018, p. 1598 ss.; C. STRINATI, *Algoritmi e decisioni amministrative*, in *Foro Amm.*, 7, 2020, p. 1591; D.-U. GALETTA, *Algoritmi, procedimento amministrativo e garanzie: brevi riflessioni, anche alla luce degli ultimi arresti giurisprudenziali in materia*, in *Riv. it. dir. pubbl. com.*, 3, 2020, p. 501 ss.

<sup>81</sup> *Ex multis* TAR Lazio, sez. III *bis*, 20 luglio 2016, n. 8312; TAR Lazio, III *bis*, 8 agosto 2018, n. 8902.

<sup>82</sup> Il riferimento è al più recente indirizzo della giurisprudenza di secondo grado (Cons. Stato, Sez. VI, 13 dicembre 2019, nn. 8472, 8473 e 8474) con la quale si è aperto all’utilizzo delle decisioni algoritmiche anche nell’ambito di attività discrezionale della pubblica amministrazione.

<sup>83</sup> Per una riflessione più attenta sul tema si veda G. GALLONE, *Blockchain, procedimenti amministrativi e prevenzione della corruzione*, cit., p. 203.

che non può che richiamare l'attenzione dello studioso dal momento che la fase di esecuzione contrattuale è quella generalmente più esposta alla permeabilità di fenomeni di tipo corruttivo<sup>84</sup>. Tale problema potrebbe tuttavia essere arginato – se non addirittura risolto – grazie a un sapiente utilizzo della *blockchain* e degli *smart contracts*<sup>85</sup>. Utilizzando tale tecnologia, infatti, sarebbe possibile limitare il potere discrezionale attribuito ai soggetti responsabili dell'esecuzione attraverso un'automazione parziale delle scelte contrattuali che generalmente presentano maggiori rischi sul versante della corruzione (per esempio subappalto e varianti in corso d'opera). Non può ignorarsi, tuttavia, che forme di ragionamento automatiche o procedurali devono essere accompagnate da concetti giuridici precisi e determinati<sup>86</sup> che non sempre ricorrono nella contrattazione pubblica. Una simile soluzione richiederebbe quindi uno studio preliminare da parte dell'amministrazione sulle più concrete modalità di attuazione.

#### 4.2 Blockchain per ridefinire l'identità digitale

Tra i vari ambiti applicativi della tecnologia *blockchain* la verifica e la gestione dell'identità digitale è forse uno dei più promettenti<sup>87</sup>. Si tratta di un tema dalle vaste implicazioni che non può tuttavia lasciare in-

<sup>84</sup> Sulla prossimità del rapporto tra contratti pubblici e corruzione si rimanda al recente contributo di F. DI LASCIO, *Anticorruzione e contratti pubblici: verso un nuovo modello di integrazione tra controlli amministrativi?*, in *Riv. trim. dir. pubbl.*, 3, 2019, p. 804 ss.

<sup>85</sup> Ai sensi dell'art. 8 *ter*, comma 2, d.l. 135/2018 «si definisce “*smart contract*” un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse». Per una panoramica generale sul tema degli *smart contracts* si veda G. GALLONE, *La pubblica amministrazione alla prova dell'automazione contrattuale. Note in tema di smart contracts*, in *Federalismi. it.*, 20, 2020, p. 142 ss.; G. MASSIMO, *La blockchain e gli smart contracts nell'innovazione del terzo millennio*, in *Dir. inform.*, 6, 2018, p. 989 ss.; F. FAINI, *Blockchain e diritto: la «catena del valore» tra documenti informatici, smart contracts e data protection*, in *Resp. civ. prev.*, 1, 2020, p. 297 ss. Sull'utilizzo degli *smart contracts* come strumento di repressione della corruzione si veda R. COUTO DE SOUZA, E. M. LUCIANO, G. WIEDENHOFT, *The use of the blockchain smart contracts to reduce the levels of corruption: some preliminary thoughts*, in *Proceedings of the 19<sup>th</sup> annual international conference of digital government research: governance in the data age*, New York, 2018.

<sup>86</sup> L. VIOLA, *Intelligenza artificiale nel procedimento e nel processo amministrativo*, cit., p. 8.

<sup>87</sup> Il rapporto tra *blockchain* e identità digitale è stato approfondito nel *report* tematico del 2 maggio 2019 dell'*EU Blockchain Observatory & Forum* della Commissione europea intitolato «*Blockchain and digital identity*», reperibile su [www.eublockchainforum.eu](http://www.eublockchainforum.eu) (visitato il 10 ottobre 2021).

differenti le istituzioni dal momento che queste, oltre a essere la fonte delle informazioni anagrafiche dei cittadini (es. certificato di nascita o di morte), devono anche preoccuparsi di poter identificare in modo preciso i suoi cittadini al pari di tutti i fruitori dei servizi pubblici da esse erogati. In un mondo ideale ogni attore dell'economia digitale dovrebbe avere un'unica e identificabile identità che possa essere provata in ogni contesto della rete, ciò senza la necessaria presenza di una terza parte e senza rivelare più informazioni di quelle richieste per la singola transazione. Tuttavia, il raggiungimento di tale obiettivo richiede il superamento dei tre ostacoli già messi a fuoco dalla Commissione europea: l'eccessiva frammentazione dell'attuale struttura dell'identità digitale, il debole collegamento tra l'identità digitale e quella "online" e la mancanza di sicurezza dei dati correlati all'identità dei cittadini<sup>88</sup>.

Non può tacersi che utilizzando gli strumenti tradizionali la risoluzione di questi problemi appare, se non impossibile, estremamente complicata. Finché la prova dell'identità richiederà la presenza di una sola entità chiamata alla raccolta delle informazioni necessarie per attestare l'identità di un individuo sarà sufficiente un singolo e ben calibrato attacco per appropriarsi dei dati di milioni di persone. La tecnologia *blockchain*, eliminando la necessaria presenza di una figura centrale, potrebbe risolvere il problema rivoluzionando il meccanismo di base che fino a oggi è stato utilizzato per provare l'identità di qualsiasi soggetto. In tal modo potrebbe avviarsi un percorso diretto al raggiungimento della *Self-Sovereign Identity* o SSI, ossia un modello di identità digitale capace di restituire al titolare il pieno controllo dei suoi dati<sup>89</sup>. La realizzazione di tale modello, oltre a garantire una maggiore protezione dei dati perso-

<sup>88</sup> Gli attacchi informatici volti all'acquisizione di dati personali (*data breach*) posseduti dalle istituzioni stanno diventando sempre più frequenti. Ad esempio, si riporta l'attacco portato a termine nel marzo del 2018 contro Aadhaar, il *database* biometrico utilizzato dall'India per identificare ogni suo cittadino, che ha portato alla sottrazione dei dati sensibili (nomi, numeri di documento e coordinate bancarie) di più di un miliardo di persone. Per un *report* interattivo su tutti i *data breach* portati a termine negli ultimi anni si rimanda a <https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks> (visitato il 10 ottobre 2021).

<sup>89</sup> La questione è stata approfondita nel *report* della Commissione europea dal titolo *SSI eIDAS Legal Report: How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market*, pubblicato nell'aprile del 2020. Tra la sterminata letteratura sul punto si veda F. WANG, P. DE FILIPPI, *Self-sovereign identity in a globalized world: credentials-based identity systems as a driver for economic inclusion*, in *Frontiers in blockchain*, 20

nali, permetterebbe al cittadino di accedere ai servizi (*account* personali, banche, servizi pubblici) con un unico *wallet*, senza al contempo fornire informazioni aggiuntive rispetto a quelle strettamente necessarie. Obiettivo, quest'ultimo, che sarà di difficile realizzazione fino a quando l'identità sarà legata a filo doppio ai documenti analogici<sup>90</sup>.

L'identità auto-sovrana forse è un orizzonte lontano, ma già diversi Paesi europei stanno testando i primi sistemi di gestione dell'identità funzionanti su *blockchain*<sup>91</sup>. Con riferimento ad ambiti più specifici, l'applicazione settoriale della tecnologia in commento che al momento sembra più promettente è sicuramente quella ricollegata al riconoscimento dei titoli di studio all'interno dell'Unione europea<sup>92</sup>; non è infatti un caso che i 30 Paesi membri della *European Blockchain Partnership* abbiano convenuto di realizzare un'infrastruttura comune dei servizi *blockchain* (EBSI) utilizzando proprio quest'ambito come caso pilota. A differenza degli altri settori di applicazione della tecnologia in esame, quello ricollegato alla certificazione dei titoli non è solo ipotetico ma è già realtà: l'Università di Milano Bicocca e l'Università di Padova hanno già sviluppato un sistema in grado di rilasciare le certificazioni di laurea tramite *blockcerts*<sup>93</sup>, mentre invece l'Università di Roma Tre ha avviato un'ambiziosa sperimentazione con l'obiettivo di creare «un fascicolo

2020; A. MÜHLE, A. GRÜNER, T. GAYVORONSKAYA, *A survey on essential components of a self-sovereign identity*, in *Computer Science Review*, 30, 2018, p. 80 ss.

<sup>90</sup> Alcune (inascoltate) soluzioni al problema dell'eccessiva diffusione dei dati relativa all'utilizzo di documenti analogici erano già state avanzate da D. BIRCH, *Psychic ID: A blueprint for a modern national identity scheme*, in *Identity in the information society*, 1, 2008, pp. 189-201 reperibile su <https://link.springer.com> (visitato il 10 ottobre 2021).

<sup>91</sup> Si riporta, ad esempio, che la città svizzera di Zug ha di recente creato delle credenziali digitali per i propri residenti utilizzando la *blockchain* Ethereum e le ha utilizzate per l'*e-voting* e per il noleggio di *e-bikes*, mentre il governo finlandese ha collaborato con una *startup* per introdurre un sistema di identificazione dei rifugiati che permette agli stessi l'utilizzo di una carta prepagata dedicata all'acquisto di cibo e altri beni di prima necessità.

<sup>92</sup> Per un approfondimento si rimanda a R. TRAINITO, M. MONACO, G. GALASSO, *Blockchain e mutuo riconoscimento dei titoli di studio nell'UE*, in *Federalismi.it*, 2, 2021, p. 167 ss.

<sup>93</sup> *Blockcerts* è uno *standard* aperto proposto dal MIT Media Lab per esprimere digitalmente un certificato e memorizzarlo su una *blockchain* in modo che sia sempre verificabile, senza necessità di interpellare l'organizzazione o la piattaforma che lo ha emesso. In altri termini, si tratta di un certificato conservato su una piattaforma *blockchain open source*.

elettronico basato sull'esperienza lavorativa, educativa, formativa che sia condivisibile tra pubblico e privato»<sup>94</sup>.

Le potenzialità della *blockchain* in questo ambito non si esauriscono tuttavia nel riconoscimento delle certificazioni ma vanno esplorate maggiormente. La Commissione europea ha indicato l'identità digitale come un «prerequisito essenziale» per l'efficienza degli Stati membri, specificando al contempo che *today's digital identity approaches are broken*<sup>95</sup>. Dal momento che la miglior candidata per intraprendere questo cambio di paradigma sembra ancora una volta la *blockchain*, non resta che attendere una presa di posizione da parte delle istituzioni italiane.

#### 4.3 Blockchain e sanità pubblica

Uno degli utilizzi più interessanti della tecnologia *blockchain* può essere riferito alla sanità pubblica<sup>96</sup>. L'impiego di tale tecnologia, infatti, potrebbe risolvere alcuni punti critici del Servizio Sanitario Nazionale (SSN) a vantaggio tanto del paziente quanto della pubblica amministrazione. Anzitutto, la *blockchain* potrebbe garantire una gestione più sicura ed efficiente delle cartelle cliniche dei cittadini, ciò in quanto allo stato attuale queste cartelle sono contenute nei *database* di singole strutture ospedaliere e la loro condivisione – che spesso avviene manualmente – appare poco efficiente e per nulla sicura. Alcuni recenti avvenimenti hanno dimostrato che attualmente le compagnie assicurative, gli ospe-

<sup>94</sup> MUR, Report *blockchain e mutuo riconoscimento dei titoli di studio nell'UE – Rapporto di Disseminazione*, Marzo 2020, p. 36 reperibile su <http://www.ponricerca.gov.it/comunicazione/publicazioni> (visitato il 10 ottobre 2021).

<sup>95</sup> *Blockchain Observatory e Forum, Blockchain and digital identity*, cit., p. 1 ss. Sul punto si veda anche il report del 7 dicembre 2018 intitolato *Blockchain for Government and Public Services*, 21-22 con cui si è sottolineato che *online identities today are also easily forged, reducing trust. Even is safe, today's paradigm – with bits and pieces of identity information saved in hundreds if not thousands of databases in all corners of the internet – is terribly inefficient and not user friendly. (...) Blockchain offers the possibility of a more fundamental fix to the digital identity problem based on turning the current paradigm on its head*.

<sup>96</sup> Le potenzialità della tecnologia *blockchain* nel campo della sanità pubblica sono state approfondite nel report tematico del 2 maggio 2019 dell'*EU Blockchain Observatory & Forum* della Commissione europea intitolato *Blockchain use cases in healthcare*, reperibile su [www.eublockchainforum.eu](http://www.eublockchainforum.eu) (visitato il 10 ottobre 2021). In letteratura, invece, tra i numerosi contributi si segnalano M. FARINA, *Blockchain e tutela della salute: verso la riorganizzazione dei sistemi sanitari?*, in *Federalismi.it*, 21, 2020, p. 170 ss.; C. PIRTLE, J. EHRENFELD, *Blockchain for healthcare: the next generation of medical records*, in *Journal of medical systems*, 42, 2018, p. 172 ss.

dali e i laboratori «siedono ciascuno sul proprio mucchio vulnerabile di dati»<sup>97</sup>. Basti pensare all'attacco cibernetico del 2016 noto come Anthem Health, che lasciò esposte le informazioni di 78 milioni di pazienti o, ancora, all'attacco sferrato l'anno successivo con un *malware* (noto come *WannaCry*) che ha criptato i file in possesso di molti ospedali chiedendo un riscatto in *bitcoin* per lo sblocco. Inoltre, in situazioni di estrema urgenza nella quale non vi è il tempo per chiedere a un'altra struttura le informazioni mediche di un paziente, questa eccessiva frammentazione delle informazioni mediche potrebbe mettere in pericolo la stessa vita del paziente (per esempio la mancata conoscenza di un'allergia a un farmaco specifico). La *blockchain* potrebbe risolvere questi problemi creando un registro sanitario decentralizzato e accessibile in qualsiasi momento e luogo da chiunque abbia il consenso – e quindi la chiave digitale – del titolare dei dati.

Le informazioni mediche, come è noto, non sono importanti esclusivamente per i pazienti. Queste, una volta rese anonime (*rectius*, pseudonimizzate) e inserite in un registro decentralizzato, potrebbero rivelarsi di centrale importanza per la ricerca. Tanto è vero che il progetto *MyHealthMyData* (MHMD), facente parte del programma UE *Horizon 2020*, intende utilizzare la *blockchain* per creare il primo *network* di informazioni biomediche europee<sup>98</sup>. I vantaggi che l'impiego di questa tecnologia emergente potrebbe apportare nell'ambito della sanità pubblica sono stati compresi anche da Paesi a noi vicini. L'Estonia, per esempio, ha riformato il suo sistema sanitario avvalendosi di un registro funzionante su tecnologia *blockchain*, così assicurando l'integrità e la sicurezza dei dati medici in esso contenuti<sup>99</sup>. Merita anche particolare attenzione il pro-

<sup>97</sup> M.J. CASEY, P. VIGNA, *La macchina della verità. La blockchain e il futuro di ogni cosa*, cit., p. 71.

<sup>98</sup> Per un maggiore approfondimento sulla struttura e sugli obiettivi di *MyHealthMyData* si rimanda a [www.myhealthmydata.eu](http://www.myhealthmydata.eu) (visitato il 10 ottobre 2021).

<sup>99</sup> La rivoluzione del sistema sanitario estone ha permesso di digitalizzare il 99% delle cartelle mediche attive, dando così la possibilità ai cittadini di accedere al loro fascicolo sanitario con un semplice *click*. I dati ufficiali sono reperibili su <https://e-estonia.com/solutions/healthcare/e-health-record/>, consultato il 10 gennaio 2021. Per un *focus* sull'esperienza estone si veda C. SULLIVAN, E. BURGER, *E-residency and blockchain*, in *Computer law & security review*, 33, 2017, p. 470.

getto svedese che prende il nome di *CareChain*, avviato con l'intenzione di implementare l'efficienza del sistema sanitario attraverso *blockchain*.

### 5. *Alcune considerazioni conclusive*

Sulla base di quanto visto nelle pagine precedenti non è possibile negare che la *blockchain* potrebbe rappresentare una valida soluzione per risolvere alcuni dei problemi strutturali della pubblica amministrazione. La rivoluzione promessa da questa tecnologia permette di immaginare un futuro non lontano in cui le pubbliche amministrazioni dei principali Stati europei possano svolgere le proprie funzioni in modo più veloce, efficiente ed efficace garantendo al contempo dei servizi pubblici ancora più vicini ai cittadini.

A queste considerazioni occorre tuttavia aggiungere che la tecnologia in commento non può essere vista come una bacchetta magica in grado di risolvere tutti i problemi che da decenni affliggono pubblica amministrazione italiana. Non deve dimenticarsi che la *blockchain* è pur sempre una tecnologia in fase di sviluppo e, almeno allo stato dell'arte, nessuno è in grado di formulare previsioni certe sul suo futuro. Quello che oggi si può intuire con assoluta certezza è che le caratteristiche dell'archetipo originario di *blockchain* ideato da Nakamoto per il funzionamento del *bitcoin* siano ontologicamente incompatibili con le caratteristiche di un'autorità pubblica. Dal momento che più ci si allontana dal modello più puro della *blockchain* e più questa sembra adatta a coadiuvare (e non a sostituire) l'amministrazione in alcuni specifici settori, le potenzialità di questa tecnologia potranno esprimersi soltanto qualora la ricerca sul campo tecnologico sia guidata e integrata dagli studiosi e operatori delle scienze giuridiche.

In Italia la diffusione di tecnologie basate su *blockchain* sta crescendo rapidamente, ma gli ultimi dati disponibili indicano che settori maggiormente interessati sono quelli della finanza, dell'agricoltura e delle catene di approvvigionamento<sup>100</sup>. Il *Digital Economy and Society Index* (DESI), strumento utilizzato dal 2014 dalla Commissione europea che mappa lo stato della digitalizzazione dell'economia dei singoli Paesi UE, ha

<sup>100</sup> Dati indicati dal report tematico *UE Blockchain Observatory and forum, EU Blockchain Ecosystem Developments*, 20 novembre 2010, p. 83.

inoltre rilevato che il settore pubblico incide solo del 4,2% sul valore di mercato della tecnologia in commento<sup>101</sup>. Gli ambiziosi obiettivi concessi dal PNRR permettono tuttavia di immaginare un'inversione di rotta che possa dare una spinta al percorso di transizione digitale che la pubblica amministrazione italiana è chiamata ad affrontare.

<sup>101</sup> *Digital Economy and Society Index (DESI)*, 2020, pp. 83-84, reperibile su <https://digital-strategy.ec.europa.eu/en/policies/desi> (visitato il 10 ottobre 2021).