

Articoli e saggi

Certezza, consenso e certificazioni informatiche: problemi e prospettive di un approccio giuridico al fenomeno delle tecnologie basate sui registri distribuiti*

Guido Befani

SOMMARIO: 1. Premesse introduttive di metodo e di contenuti. – 2. Le tecnologie basate sui registri distribuiti nella realtà economica: il caso *blockchain*. – 3. Inquadramento normativo, definizione ed effetti giuridici. – 4. Questioni giuridiche aperte dalla *blockchain*: è tutto oro quello che luccica? – 5. Pubblico e privato nell'attività di certificazione: l'aporia cripto-anarchica dell'informatica. – 6. La notarizzazione impossibile: il problema dei generali bizantini tra consenso, accertamenti fattuali e potestà pubblicistiche. – 7. Verso una rilettura analogica delle funzioni di *hash*: le certezze pubbliche del “notaro dell'avvenire”. – 8. Lo stato dell'arte negli altri Paesi: l'incompiuta regolazione del fenomeno. – 9. Considerazioni conclusive.

1. *Premesse introduttive di metodo e di contenuti*

L'ultimo stadio evolutivo del progresso tecnologico, come è noto, ha visto applicare le funzioni crittografiche di *hash* ai documenti digitali, nel tentativo, sicuramente affascinante, di risolvere un problema molto sentito dell'informatica, cioè quello di fornire unicità ai “valori digitali” per evitare sia manipolazioni del contenuto dei *file*, sia il fenomeno della loro “doppia alienazione”(c.d. *double spending*).

Nell'*idem sentire* della comunità informatica, infatti, le transazioni di valori digitali validate e registrate ricorrendo alle tecnologie basate sui registri distribuiti, le c.d. *blockchain*, godono di una presunzione di “certezza”, unicità e immutabilità che però, al netto dei potenziali risvolti pratico-operativi, ancora tutti da

* Il presente contributo è stato realizzato nell'ambito del progetto di ricerca “*Internet Of Things (IoT) e Blockchain: ricerca, design e sviluppo di soluzioni per il mercato*” (IoT&B), CUP: J48C17000230006 - Responsabile Scientifico: Prof. Gianfranco d'Atri.

esplorare, iniziano a ingenerare degli inevitabili interrogativi di ordine giuridico-sistematico, sia sull'astratta ammissibilità di un simile supporto documentale nell'ambito di un ordinamento giuridico "tecnologicamente neutro"¹, oltretutto improntato alla libertà delle forme, sia sugli eventuali effetti giuridici da riconoscere a un simile "sigillo digitale" nel contesto normativo di un sostanziale vuoto regolamentare.

In questo senso, l'analisi giuridica dei quesiti sollevati dalla *blockchain* non può prescindere da un approccio necessariamente interdisciplinare, ponendo al centro della riflessione e dell'inevitabile dibattito il necessario incontro di prospettiva, e quindi di visuale, tra l'informatico e l'amministrativista².

Infatti, a fronte dell'eterogeneità di un fenomeno inevitabilmente complesso – quale è l'impatto potenziale della *blockchain* nelle transazioni digitali – sarà possibile ottenere uno spettro d'indagine metodologicamente più strutturato e approfondito solo attraverso le differenti modalità di "messa a fuoco" che intercorrono tra informatica e diritto, con una visione prospettica d'insieme che sia polarizzata nei due punti di fuga della "tecnica" e della "norma".

La necessaria convergenza scientifica tra le diverse discipline è ancor più evidente se solo si considera che, nei differenti linguaggi scientifici e terminologie descrittive della *blockchain*, gli stessi concetti di "pubblico" e "privato" applicabili alle tecnologie basate sui registri distribuiti, appaiono diametralmente invertiti e generano non pochi imbarazzi ermeneutici tra informatici e giuristi.

Non è quindi un caso che, sotto la supervisione scientifica del Prof. Danilo Pappano (amministrativista), il presente contributo si inserisce nell'ambito del progetto di ricerca multidisciplinare "*Internet Of Things (IoT) e Blockchain: ricerca, design e sviluppo di soluzioni per il mercato*", nel quale, il responsabile scientifico Prof. Gianfranco d'Atri (matematico), ha coinvolto nella riflessione di più ampio respiro delle realtà scientifiche tra di loro eterogenee che spaziano dall'informatica, al diritto, dalla matematica alla filosofia, perché i maggiori interroga-

¹ Nell'economia del presente contributo, sulla "neutralità" del diritto rispetto alla tecnologia, si rinvia *ex multis* G. Finocchiaro, *Riflessioni su diritto e tecnica*, in *Dir. inf. e inform.*, 2012, 4-5, 831 s., la quale rileva come «I vantaggi della neutralità tecnologica sono evidenti: il diritto non condiziona il mercato, favorendo questa o quella tecnologia; non condiziona lo sviluppo della tecnica; non deve rincorrerla. L'approccio del diritto, nella neutralità tecnologica, è "funzionale". Non si concentra sul "cosa", ma sul "come". Legiferare in questo modo può essere più difficile, perché non si norma l'oggetto, ma la funzione». Sul medesimo tema, più diffusamente cfr. *infra*, nota seguente e il par. 9.

² Come è stato osservato, infatti, «Il confronto con il progresso tecnico-scientifico è divenuto un problema centrale anche per l'amministrazione pubblica e il diritto amministrativo». Sul punto, cfr. S. Civitarese Matteucci, L. Torchia (a cura di), *La tecnicizzazione*, in L. Ferrara, D. Sorace (a cura di), *A 150 anni dall'unificazione amministrativa italiana. Studi*, vol. IV, Firenze, 2016, 7. In termini più generali, la messa a fuoco sulla relazione che intercorre tra diritto e tecnica, e sulla strumentalità dell'uno rispetto all'altro, è al centro del noto dialogo tra Irti e Severino, cui si rinvia a N. Irti, E. Severino, *Dialogo sul diritto e tecnica*, Bari, 2001, nonché a L. Mengoni, *Diritto e tecnica*, in *Riv. trim. dir. e proc. civ.*, 2001, sulla "dominazione" del diritto sulla tecnica.

tivi sollevati dalle nuove tecnologie, al netto delle evidenti e doverose divergenze scientifiche di approccio, appaiono sintetizzarsi nell'ambito operativo della produzione di "certezze relazionali".

Proprio il filone di ricerca legato all'affidabile "certezza" di queste tecnologie, sta rispolverando un certo fascino di indagine para-antropologica per la scienza gius-pubblicistica, di indiscutibile interesse per gli studiosi del diritto amministrativo³, al fine di provare a riportare un doveroso ordine concettuale alle eccessive fughe in avanti della tecnologia. E lo stesso concetto di certezza, come è stato già osservato dalla dottrina, «è carico di significati e di ambiguità»⁴ e, nell'attuale enfasi pan-digitale, per gli studiosi del diritto si aprono diversi interrogativi sull'astratta ammissibilità di questa asserita funzione certificativa, digitalmente distribuita, che vorrebbe scardinare l'idea stessa di un soggetto istituzionalmente fidefaciente nell'ideale di creare "fiducia attraverso la disintermediazione", inserendosi di soppiatto nella progressiva e costante evoluzione informatica che ha comportato una sua sempre maggiore applicazione nei rapporti economici e negli apparati produttivi, segnando il definitivo passo di transizione da un sistema "analogico" al nuovo mondo digitale. Questo fenomeno, che in una prospettiva di una maggiore celerità dell'azione pubblica e dei rapporti intersoggettivi, specialmente con i cittadini e le imprese, ha interessato anche l'operato della P.A. sull'abbrivio della notoria "tele-amministrazione" degli anni '90⁵, impone una più attenta riflessione ispirata a delle fondamentali esigenze di contenimento di eccessive fughe in avanti, legittimate da una tendenziale sfiducia nei confronti di un'autorità accentratrice e che trovano, in un contesto ordinamentale di sostanziale vuoto normativo, terreno fertile dove poter germogliare.

Con queste inevitabili premesse, quindi, l'obiettivo che il presente contributo si prefigge è rappresentato dalla ricerca, *iure condito*, di un possibile inquadramento giuridico della *blockchain* che vada oltre la semplice lettura dell'art. 8-ter del d.l. 14 dicembre 2018, n. 135, cercando di coglierne la vera essenza giuridica del fenomeno al netto degli attuali limiti normativi, soprattutto in un panorama comparato tutt'altro che uniforme. Presupposto indispensabile dell'analisi pro-

³ In questo senso, si veda la sempre attuale definizione di Giannini della "certezza pubblica", quale strumento preordinato ad attestare *erga omnes* la realtà di alcuni fatti giuridicamente rilevanti. Sul punto, M.S. Giannini, *Certezza pubblica*, in *Enc. dir.*, vol. VI, Milano 1960, 769 s.

⁴ A. Fioritto, *La funzione di certezza pubblica*, Padova, 2003, 1.

⁵ In forza del principio *digital first* che ha imposto già a livello europeo la massima digitalizzazione dell'attività amministrativa, a partire dagli anni '90, nell'alveo delle riforme apportate dalle c.d. Leggi Bassanini, la P.A. ha seguito nel processo di informatizzazione attraverso la gestione del procedimento amministrativo attraverso i sistemi telematici, la c.d. "tele-amministrazione". Nell'economia del presente lavoro, si rinvia per gli opportuni approfondimenti a G. Duni, *Teleamministrazione*(voce), in *Enc. giur.*, vol. XXX, 1994; alle considerazioni di N. Irti, *Idola Libertatis*, Milano, 1985 (spec. 74); A. Masucci, *Il documento informatico*, in Aa.Vv., *La documentazione amministrativa*, Rimini, 2001, 211 s., nonché a F. Costantino, *Autonomia dell'amministrazione e innovazione digitale*, Napoli, 2012.

posta, pertanto, è la ricostruzione delle categorie di teoria generale applicabili alle tecnologie basate sui registri distribuiti⁶, sulla scia del sempre attuale e ambizioso insegnamento di Carnelutti, per il quale «una teoria generale del diritto dovrebbe essere, nientemeno, una rappresentazione del mondo»⁷. In questo senso, un sentito ringraziamento va al collega assegnista di ricerca, Enrico Zanardo (informatico), per gli interessanti e imprescindibili spunti di riflessione pratico-operativi delle funzioni crittografiche di *hash* e dei meccanismi informatici di ricerca del c.d. “consenso” tra i vari nodi della rete.

Laddove possibile, nel circoscrivere l'analisi al tema proposto, escludendo in questa sede qualsiasi approfondimento in merito all'eventuale applicabilità della tecnologia alla semplificazione amministrativa⁸, ovvero alla tematica dei c.d. *big data*⁹, si cercherà di cogliere le prospettive di implementazione della *blockchain* in funzione certificativa, in termini di effettiva “certezza legale”¹⁰ e fidejussione generalizzata.

2. *Le tecnologie basate sui registri distribuiti nella realtà economica: il caso blockchain*

Nella vergine foresta del linguaggio, da un punto di vista meramente descrittivo, la *blockchain* può essere unitariamente definita come una struttura tecnologica di registrazione di dati distribuita e immodificabile¹¹.

⁶ Si veda a tal proposito, l'assunto di S. Pugliatti, *La logica e i concetti giuridici*, in *Riv. dir. comm.*, 1941, 199, per il quale «l'ordinamento giuridico può esaurire tutta la realtà possibile solo in quanto sia una unità sistemica, per ciò stesso concretamente inesauribile; come disorganica pluralità, non potrebbe andare oltre la puntuale corrispondenza tra il caso concreto e la norma espressa, e sarebbe dunque tutto contenuto nei modesti limiti delle specifiche previsioni».

⁷ F. Carnelutti, introduzione a *La prova Civile*, Milano, 1947, 7.

⁸ In questo senso, al di là di ogni ulteriore considerazione critica sull'astratta possibilità di riconoscere alla *blockchain* un ruolo nella semplificazione amministrativa, nell'economia del presente contributo, si rinvia per gli opportuni approfondimenti al numero monografico di www.federalismi.it, n. 2/2021, *Blockchain, politiche pubbliche, regole. Dalle semplificazioni amministrative alla digitalizzazione*, nonché, con particolare riferimento alla semplificazione amministrativa, a M. Macchia, *Blockchain e pubblica amministrazione*, ivi, 117 s.

⁹ Per l'approfondimento delle maggiori problematiche giuridiche connesse con l'impiego massivo dei c.d. *Big Data*, senza alcuna pretesa di completezza, si rinvia a G. Olivi, “*Big Data*”, *metadati e Intelligenza Artificiale: i confini tra i diversi diritti*, in *Il Diritto industriale*, 2020, 2, 181 s.; M. Palmirani, “*Big Data*” e *conoscenza*, in *Riv. fil. dir.*, 2020, 1, 73 s.; nonché G. De Minico, “*Big Data*” e *la debole resistenza delle categorie giuridiche. “Privacy” e “lex mercatoria”*, in *Dir. pubbl.*, 2019, 1, 89 s.

¹⁰ Come rilevato da M.S. Giannini, op. cit., le certezze che producono situazioni oggettive o soggettive, le quali interessino tutti o determinati soggetti, appartengono al gruppo delle certezze legali, e sono indubbiamente più interessanti. Il potere che si riserva lo Stato di produrre certezze legali – potere certativo – dà luogo ad una funzione pubblica.

¹¹ Come è noto, il concetto di *blockchain* come sistema di gestione di un registro distribuito è stato descritto per la prima volta nel 2008, vero o pseudonimo che sia, da Satoshi Nakamoto nel *white paper* “*Bitcoin: A Peer-to-Peer Electronic Cash System*” da questo schema iniziale di *blockchain* basata sullo scambio di *bitcoin*, si sono generate diverse altre tipologie di *blockchain*.

Già dalla sua traduzione letterale di “catena di blocchi”, infatti, è possibile ricavare la sua essenza di un registro digitale, nel quale le singole voci ivi trascritte, attraverso un “marcatore temporale”¹², sono cronologicamente ordinate in “blocchi concatenati” e l’integrità dei quali è garantita dall’impiego di un sistema di crittografia¹³ che, a livello informatico, “traduce” in stringhe alfanumeriche qualunque documento, immagine o foglio di testo. Questa operazione è conosciuta come *hashing*.

Premesso che esistono varie categorie di *blockchain*, declinabili in base all’accesso più o meno ampio in “pubbliche” e “private”¹⁴, ovvero sulla maggiore o minore libertà di validazione per gli utenti qualificati, i c.d. minatori¹⁵, il profilo di maggior interesse per il giurista che intenda indagare sul fenomeno con un approccio laico, e al netto di eccessive contaminazioni inter-disciplinari, è rappresentato dalla circostanza che, attraverso le funzioni crittografiche di *hash*¹⁶, è possibile attribuire a ogni *file* con un determinato contenuto grafico, un’univoca “impronta digitale” – nel senso anatomico del termine – e di far sì che una molteplicità di dati possano essere tradotti e trascritti in blocchi (*block*) che saranno poi collegati tra loro per formare una catena (*chain*) la quale, una

¹² C.d. *timestamping*.

¹³ I sistemi a crittografia asimmetrica utilizzano “chiavi” diverse per criptare e decriptare il messaggio, la prima chiave per criptare è di dominio pubblico per tutti gli utenti della piattaforma, la seconda, invece è privata. Per completezza espositiva, sebbene la crittografia sia antica quanto la scrittura stessa, occorre evidenziare come il principio della crittografia a chiave pubblica sia un’ideazione abbastanza recente, elaborata nel 1976 dagli studiosi dell’Università di Stanford Whitfield Diffie e Martin L. Hellmann. L’anno successivo, in seno al MIT di Boston, il sistema è stato ulteriormente implementato da Ronald L. Rivest, Adi Shamir e Leonard M. Adleman, ideatori del più noto algoritmo RSA. Nell’economia del presente contributo, si rinvia per ulteriori approfondimenti a C. Paar, J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioner*, Springer, 2010.

¹⁴ Si definiscono “pubbliche” le piattaforme *blockchain* senza alcuna restrizione di accesso dove “chiunque” può operare ottenendo una copia del registro, il c.d. *ledger*; “ibride” le piattaforme parzialmente decentrate strutturate con un controllo sul consenso sulle transazioni attraverso una serie di nodi preselezionati, e “private” le infrastrutture centralizzate con delle limitazioni all’accesso a determinati utenti qualificati e dove le operazioni di scrittura sono ristrette. La distinzione sostanziale, tra le tre categorie, è data dal meccanismo di “consenso” sulle operazioni e al differente grado di accessibilità. Sul punto, cfr. più diffusamente *infra*, par. 6.

¹⁵ I minatori, o *miners*, sono degli utenti qualificati che prestano il potere computazionale delle proprie macchine per svolgere i calcoli necessari a concludere un blocco di operazioni da aggiungere alla catena. A seconda, quindi, dell’eventuale autorizzazione necessaria a costoro per poter operare, si avrà un’ulteriore suddivisione in *permissionless blockchain*, dove chiunque può partecipare come utente *standard* o come *miner*, e *permissioned blockchain* nel caso in cui la possibilità di operare come *miner* è rimessa all’apprezzamento di un’entità centrale.

¹⁶ L’impiego delle funzioni crittografiche di *hash* generano come risultato dei numeri di elevata grandezza attraverso il noto codice binario 0-1, garantendo la “quasi” impossibilità di collisione, cioè di avere lo stesso numero associato a due processi crittografici differenti. La caratteristica fondamentale di queste funzioni risiede infatti nella loro invertibilità: in questo modo, dato un determinato valore di *hash* in uscita, non solo è matematicamente “impossibile” risalire al messaggio che l’ha generato, per mancata iniettività della corrispondenza, ma è anche computazionalmente inverosimile trovare un messaggio diverso dall’originale che produca la stessa stringa predeterminata.

volta “confermata”¹⁷ non consentirà più alcuna modifica retroattiva dei contenuti in un determinato blocco, senza dover modificare anche i precedenti, perché ogni minima modifica successivamente apportata al documento, immagine o testo “tradotto” produrrà una diversa stringa alfanumerica di uscita.

Pertanto, quello che davvero interessa (o per lo meno dovrebbe interessare) il giurista, è l’astratta possibilità di impiegare questa tecnologia per risolvere i conflitti interpretativi sulla certezza delle transazioni, perché attraverso l’*hashing* sarà possibile verificare che, tra un passaggio di mano e l’altro, l’elemento trascritto nel registro digitale sia esattamente lo stesso, senza subire alterazione alcuna rispetto alla versione originale¹⁸.

Nella sostanza, come già evidenziato nelle premesse introduttive, l’infrastruttura crittografica offerta dalla *blockchain* vorrebbe rappresentare il tentativo di far raggiungere il consenso in merito all’unicità dei valori digitali per evitare il fenomeno della “doppia alienazione” nei vari passaggi e transazioni che i vari nodi appartenenti al network analizzano. Il tutto, si badi bene, senza interporre la figura di un terzo “fiduciario” chiamato a svolgere la funzione di intermediario qualificato.

Secondo l’ideologia cripto-anarchica¹⁹ ispiratrice della più conosciuta *bitcoin-blockchain*, infatti, l’aver predisposto un’architettura informatica decentralizzata e distribuita ingenererebbe un sistema di controllo diffuso da parte degli utenti che, di fatto, minimizzerebbe il rischio di manipolazioni dei contenuti, posto che non sarebbe possibile che un singolo utente, i.c.d. *miner* (o un gruppo di utenti che non rappresenti la maggioranza degli operatori sulla piattaforma) possa influenzare il meccanismo di validazione dei blocchi²⁰.

¹⁷ Affinché la validazione di ciascun blocco diventi effettiva, è necessario che i *miner* risolvano un problema crittografico attraverso il c.d. *proof of work*, risolto il quale ricevono una ricompensa. Cfr. sul punto, M. Giuliano, *La blockchain e gli smart contracts nell’innovazione del diritto nel terzo millennio*, in *Dir. inf. e inform.*, 2018, 989 ss.

¹⁸ Nello specifico, poiché ogni stringa di *hash* contiene l’*hash* del blocco precedente, qualsiasi tentativo di modifica unilaterale e retroattivo comporta la modifica dell’*hash* successivo provocando una sorte di “rottura”, *rectius* biforcazione della catena su un doppio binario, madre e derivato. In questo senso, poiché anche la “rettifica” dei dati è difficilmente esercitabile in via retroattiva, il rimedio pratico è offerto dalla generazione di un nuovo blocco rettificato.

¹⁹ Come è noto, l’evoluzione delle potenzialità della rete ha comportato l’insorgere del fenomeno del c.d. cripto-anarchismo, quale ideale volto alla realizzazione della piena libertà di movimento e di espressione grazie all’anonimato digitale reso possibile dai sistemi crittografici.

²⁰ Tutti i nuovi blocchi, infatti, poiché per essere trascritti nella *blockchain* sono generati utilizzando una procedura di “consenso” informatico previsto dall’algoritmo, il c.d. *Proof of Work* è la procedura più diffusa per stabilire il consenso, assieme alla *Proof of Stake*, *Proof of Capact*, *Proof of Burn*, *Proof of Activity*. In questo senso, l’immodificabilità dei dati va intesa dal punto di vista unilaterale, laddove un solo utente non ha modo di apportare modifiche se non a maggioranza. Ogni modifica, infatti, è soggetta all’approvazione consensuale degli operatori sui nodi, secondo le “regole” informatiche del consenso. A causa della successiva memorizzazione dei dati in una *blockchain*, questi non possono essere modificati successivamente senza danneggiare l’integrità dell’intero sistema. Ciò rende la manipolazione dei dati molto più difficile. Il meccanismo di consenso decentralizzato

L'asserita inalterabilità delle operazioni, a cui si somma la carenza di un chiaro centro di potere, farebbe perciò sì che, una volta che la transazione sia stata autorizzata dal sistema e aggiunta al blocco, la stessa non sia più annullabile o modificabile, se non per mezzo di separata operazione, identica ed opposta, effettuata successivamente con il consenso di tutti (o quasi) i partecipanti. Come si vedrà²¹, infatti, proprio sui meccanismi di ottenimento del consenso permangono le diverse criticità delle infrastrutture informatiche di "governo" della *blockchain*, che rischiano di compromettere quell'aura di affidabilità assoluta della macchina, da privilegiare alla malizia dell'uomo.

Obiettivamente, ad una prima lettura, il vantaggio della crittografia delle funzioni di *hash*, unite alla distribuzione simultanea del supporto di scrittura del registro, sembrerebbero consentire un incondizionato potenziale di affidabilità sulla circolazione dei dati trascritti. Tuttavia, sia il quadro regolatorio, tanto a livello nazionale quanto in chiave comparata, sia diverse ombre di matrice giuridico-tecnologica, non offrono significativi margini di manovra per riconoscere un'effettiva valenza generalizzata di "certezza" nel senso giuridico del termine.

3. *Inquadramento normativo, definizione ed effetti giuridici*

Nonostante la tecnologia *blockchain* sia già alla base di numerose applicazioni pratico-operative che hanno suscitato un vivo interesse per gli operatori di mercato, quali, in ordine sparso, criptovalute; *smart contract*; certificazione dati; pubblicità digitale; identità digitale; piattaforme di pagamento elettronico, piattaforme di voto elettronico, l'effettivo inquadramento giuridico non è del tutto chiaro e scevro da pericolose zone d'ombra²².

Nell'ordinamento giuridico italiano, la definizione di *blockchain*, è offerta dall'art. 8-ter del d.l. 135/2018, c.d. Decreto Semplificazioni, il quale definisce "Tecnologie basate su registri distribuiti" le tecnologie e i protocolli informatici che «usano un 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 sia in chia-

sostituisce la necessità di una terza parte affidabile per confermare l'integrità delle transazioni. Come evidenziato in nota precedente, non sono infrequenti le biforcazioni dei nodi laddove non sia stato possibile comporre le divergenze di "consenso", la struttura della *blockchain* si scinde in due entità distinte, governate da regole diverse. Cfr. sul punto U. Bechini, *Da Berlino a Dublino e Pechino: sulle tracce della Blockchain*, in *Riv. not.*, 2018, 6.

²¹ Sui profili critici del raggiungimento del consenso, cfr. più diffusamente *infra*, par. 6.

²² Cfr. E. La Sala, *L'applicazione della "Distributed Ledger Technology" all'emissione di strumenti finanziari di debito*, in *Le Società*, 2019, 6, 715 s.

ro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili».

A dispetto dell'apparente linearità della definizione, ancora una volta²³, il legislatore nazionale non ha offerto alcuna connotazione giuridico-sistemica per inquadrare correttamente questa tecnologia con dei significativi margini di consapevolezza, anzi, diversi sono i risvolti critici ai quali la norma presta inevitabilmente il fianco²⁴.

L'art. 8-ter del Decreto Semplificazioni, infatti, al comma 3, si limita a riconoscere che la memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti «produce gli effetti giuridici della validazione temporale elettronica»²⁵ di cui all'art. 41 del Regolamento (UE) n. 910/2014, c.d. Regolamento eIDAS.

A fronte di questo rimando normativo, pertanto, l'effetto giuridico riconosciuto si sostanzierebbe unicamente nell'equiparare l'utilizzo della tecnologia basata sui registri distribuiti alla "validazione temporale elettronica", rispetto alla quale, il comma 1 dell'art. 41 ivi richiamato, dispone che «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 temporale elettronica qualificata»²⁶.

La scelta normativa di equiparare la *blockchain* alla validazione temporale elettronica "semplice", lascerebbe perciò intendere l'espressa esclusione degli ulteriori effetti riconosciuti dalla validazione temporale elettronica "qualificata", alla quale, invece, il comma 2 dell'art. 41 del Regolamento eIDAS riconosce la

²³ La tendenza legislativa di prevedere definizioni non-giuridiche ai fenomeni nuovi è cosa ben nota. In tal senso si vedano le considerazioni critiche già svolte sulla definizione non-giuridica di criptovaluta offerta dal d.lgs. 90/2017, per le quali sia consentito un rinvio al mio *Contributo allo studio sulle criptovalute come oggetto di rapporti giuridici*, in *Dir. econ.*, 3, 2019, 203 s. Con specifico riferimento al decreto semplificazioni, qui in commento si vedano altresì i rilievi critici di C. Bomprezzi, *Commento in materia di Blockchain e Smart contract alla luce del nuovo Decreto Semplificazioni*, in *Dir. merc. tecn.*, 2019, 1-7, il quale stigmatizza le maggiori criticità sulle definizioni imprecise e sulla sostanziale superfluità delle disposizioni che rischiano di limitare l'implementazione tecnologica in luogo di incentivarla.

²⁴ Per un commento critico al decreto semplificazioni, si vedano, oltre a Bomprezzi, *op. cit.*; anche Sarzana di S. Ippolito, *Blockchain e smart contract nel nuovo decreto semplificazioni*, in *Dir. Internet*, 2019, 17.

²⁵ Secondo la definizione offerta dal regolamento, la validazione temporale elettronica, è intesa come un complesso di dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento. La prima forma di *timestamping* di cui si ha notizia è quella elaborata da S. Haber, W. Scott Stornetta, *How to Time-Stamp a Digital Document*, *Journal of Cryptology*, 1991.

²⁶ Ai sensi dell'art. 42 Regolamento (UE) n. 910/2014, la validazione temporale elettronica qualificata deve soddisfare i seguenti i requisiti: a) collega la data e l'ora ai dati in modo da escludere ragionevolmente la possibilità di modifiche non rilevabili dei dati; b) si basa su una fonte accurata di misurazione del tempo collegata al tempo universale coordinato; e c) è apposta mediante una firma elettronica avanzata o sigillata con un sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato o mediante un metodo equivalente.

«presunzione²⁷ di accuratezza della data e dell'ora che indica e di integrità dei dati ai quali tale data e ora sono associate», lasciando, pertanto, al libero apprezzamento del giudice la valutazione sull'ammissibilità probatoria della validazione "semplice".

A giudizio di chi scrive, tuttavia, la scelta legislativa enucleata nella dubbia formulazione letterale dell'art. 8-ter, si tradurrebbe in un sostanziale vuoto regolamentare, atteso che, senza considerare le specificità già esistenti nell'ordinamento per l'acquisizione delle prove digitali nel processo penale²⁸, qualsiasi supporto documentale rappresentativo di un fatto può essere prodotto come prova anche nel giudizio civile²⁹ o nel processo amministrativo³⁰, laddove l'unico aspetto di maggior rilievo, semmai, è dato dalla marcatura temporale, cioè da quel servizio offerto da un "Certificatore accreditato"³¹ che consentirebbe di associare a un documento informatico data e ora certe, legalmente valide e opponibile a terzi.

²⁷ Nell'ambiguità definitoria della norma, appare preferibile l'impostazione metodologica di ritenerla una presunzione relativa, ben potendo essere ammessa prova contraria. Sulla presunzione, in termini generali, si rinvia a M. Taruffo, *Certezza e probabilità nelle presunzioni*, in *Foro it.*, 1974, V, 83 s.; nonché V. Andrioli, *Presunzioni (Diritto civile e Diritto processuale civile)*, in *Noviss. dig. it.*, vol. XIII, Torino, 1966, 766 s.

²⁸ In questo seno, con specifico riferimento al processo penale, si vedano gli artt. 244, 247 e 354 c.p.p., come modificati dalla l. 18 marzo 2008, n. 48, di ratifica ed esecuzione della Convenzione di Budapest sulla criminalità informatica, i quali disciplinano già i casi di ispezione, perquisizione e accertamento urgente aventi ad oggetto dati, informazioni, programmi informatici o sistemi informatici o telematici. Ai fini dell'ammissibilità della prova digitale nel processo, pertanto, sono richieste misure tecniche idonee alla garanzia di conservazione dei dati conformemente all'originale informatico. Sul punto, cfr. R. Brighi, V. Ferrari, *Digital evidence e tutele processuali: potenzialità della tecnologia blockchain*, in *Ragion pratica*, 2018, 2.

²⁹ Si veda, al riguardo, la sempre attuale elaborazione scientifica di F. Carnelutti, in *La prova civile*, Roma, 1947, 140, nonché Id., *Torniamo al «giudizio»*, in *Riv. dir. proc.*, 1949, I, 165 s, laddove con una ricchezza di prospettive e di lucidità di approfondimento, rileva, in riferimento alla prova documentale, come il "documento" altro non sia che una «cosa rappresentativa, cioè capace di rappresentare graficamente un fatto». L'economia del presente contributo non consente un'esauriva trattazione di tutte le riflessioni giuridiche della dottrina sul concetto di "prova", che trova forse una migliore *sedes materiae* nelle trattazioni processualistiche e di diritto penale. Sul punto, senza alcuna pretesa di completezza su di un tema così vasto, si rinvia ad A. Giuliani, *Il concetto di prova. Contributo alla logica giuridica*, Milano, 1961; S. Pugliatti, *Conoscenza*, in *Enc. dir.*, vol. IX, Milano, 45 s.; P. Calamandrei, *Verità e verosimiglianza nel processo civile*, in *Opere giuridiche*, I, Napoli, 1965, 624, s.; G. Verde, *Prova (teoria gen. e dir. proc. civ.)*, in *Enc. dir.*, vol. XXXVII, Milano, 1988; M. Pisani, *Intorno alla prova come argomentazione retorica*, in *Riv. dir. civ.*, 1959, I, 458 s.; M. Taruffo, *Prove atipiche e convincimento del giudice*, in *Riv. dir. proc.*, 1973, 389 s.; Id., *Studi sulla rilevanza della prova*, Padova, 1970.

³⁰ A fronte del noto rinvio esterno al c.p.c. operato dall'art. 39 c.p.a., a mente del quale, per quanto non disciplinato dal codice «si applicano le disposizioni del codice di procedura civile, in quanto compatibili o espressione di principi generali».

³¹ Nello specifico, qualora i prestatori di servizi fiduciari – c.d. Trust Service Providers – intendano offrire la prestazione di un servizio fiduciario qualificato, hanno l'obbligo di trasmettere all'AgID, quale organismo di vigilanza, l'intenzione di "avviare un servizio fiduciario qualificato", doverlo allegare anche una relazione di valutazione di conformità, c.d. *ConformityAssessment Report*, rilasciata da un organismo di valutazione di conformità, c.d. *ConformityAssessment Body*, accreditato da organismi di accreditamento riconosciuti dagli Stati membri (ETSI EN 319 403). Cfr. https://www.etsi.org/deliver/etsi_en/319400_319499/319403/02.02.02_60/en_31-9403v020202p.pdf

Come già rilevato dalla dottrina³², infatti, la *blockchain*, ancorché faccia uso di soluzioni tecnologiche proprie della firma digitale, non soddisferebbe i parametri e requisiti normativi richiesti dal Regolamento eIDAS e dal Codice dell'Amministrazione digitale in ordine alla validazione temporale elettronica³³ e alla certificazione dell'identità digitale³⁴.

Oltretutto, il comma 4 dell'art. 8-ter, aveva demandato all'Agenzia per l'Italia digitale, entro novanta giorni dalla data di entrata in vigore della legge di conversione 11 febbraio 2019, n. 12, di individuare gli *standard* tecnici che le tecnologie basate su registri distribuiti debbono possedere ai fini della produzione dei menzionati effetti giuridici.

A tutt'oggi (novembre 2020 n.d.a.), l'Agenzia per l'Italia digitale non ha individuato gli *standard* tecnici che le tecnologie basate su registri distribuiti debbano possedere ai fini della produzione degli effetti di cui al comma 3 dell'art. 8-ter del d.l. 135/2018, lasciando insoluto il problema sull'effettiva valenza giuridico-certificativa della *blockchain*, il quale, al netto di ogni possibile approccio tecnologico perseguibile dall'AgID, non sembrerebbe essere solo di natura informatica.

Nel mese di giugno 2020, infatti, nel tentativo di dotare il Paese di un quadro regolamentare competitivo nei confronti degli altri Paesi, è stata lanciata dal Ministero per lo sviluppo economico una consultazione pubblica sulle «Proposte per la Strategia italiana in materia di tecnologie basate su registri condivisi e Blockchain», un documento programmatico di sintesi e discussione sulle potenzialità della tecnologia, senza però offrirne alcuna qualificazione o connotazione giuridico-sistematica, limitandosi a raccomandare la ricerca di «certezza giuridica e regolamentazione efficace, che consentano di sostenere l'innovazione e trarre vantaggio dallo sviluppo tecnologico, proteggendo al contempo gli interessi generali e più ampi della società».

L'iniziativa italiana in materia di *blockchain*, in ultima analisi, vorrebbe avere il presupposto ideologico di integrarsi con le politiche dell'Unione Europea in materia³⁵. Tuttavia, al netto di ogni considerazione sull'opportunità di un quadro regolatorio unico che sia di stimolo e incentivo, è un dato di fatto come, a livello europeo, manchi ancora uno strumento di diritto derivato che possa offrire un

³² M. Giuliano, *op. cit.*

³³ Le marcature temporali, infatti, sono un servizio offerto da un "Certificatore accreditato", che consente di associare ad un documento elettronico data e ora certe, legalmente riconosciute, e opponibili a terzi. Le marcature temporali, inoltre, non sarebbero emesse da un Prestatore di Servizi Fiduciari così come previsto nel Regolamento eIDAS, ma ciascun blocco contiene un riferimento temporale svincolato da qualsiasi parametro di accuratezza.

³⁴ Allo stato attuale, infatti, gli operatori di una piattaforma *blockchain* possono operare in un totale (o quasi) anonimato.

³⁵ Si veda, a tal proposito, l'adesione dell'Italia alla *European Blockchain Partnership*, l'iniziativa multilaterale governativa di collaborazione tra gli stati membri per lo scambio di esperienze sul piano tecnico e regolatorio.

parametro giuridico comune agli Stati membri. Nondimeno, le diverse prese di posizione delle istituzioni, come si vedrà³⁶, se da un lato “strizzano l’occhio” alle potenzialità della tecnologia (a partire dalla Commissione europea³⁷), dall’altro, evidenziano alcune preoccupazioni sull’utilizzo inconsapevole di un simile strumento³⁸, lasciando sostanzialmente mano libera ai governi nazionali di procedere in ordine sparso.

4. *Questioni giuridiche aperte dalla blockchain: è tutto oro quello che luccica?*

L’introduzione delle tecnologie basate sui registri distribuiti nella realtà economica, se da un lato suscita grandi attrattive futuristiche di digitalizzazione dei processi produttivi, corroborati da ipotetiche garanzie di tracciabilità assolute, dall’altro rischia di ampliare il novero delle problematiche giuridiche da risolvere, piuttosto che porvi rimedio.

Come già riconosciuto dal Ministero per lo sviluppo economico³⁹, al netto di ogni ulteriore profilo pratico-operativo di possibile impiego, la principale e potenziale caratteristica offerta da questa tecnologia, infatti, è quella di ambire aridurre, in alcuni casi anche drasticamente, il costo della fiducia necessario al perfezionamento di una transazione, garantendo al tempo stesso “certezza” della sua esecuzione in tutti quei contesti in cui il costo della fiducia è una componente rilevante del costo transazionale (si pensi al settore bancario, assicurativo, immobiliare, alla tracciabilità della filiera agro-alimentare o all’*expertise* di opere d’arte⁴⁰).

³⁶ Cfr. più in dettaglio *infra*, par. 9.

³⁷ Si veda in tal senso la Comunicazione della Commissione Europea del febbraio 2020 “*Shaping Europe’s digital future*” con la quale è stata ribadita l’importanza della *Blockchain* inserendola fra le *key action* per il secondo trimestre del 2020, nonché l’iniziativa avviata diretta alla creazione di una rete infrastrutturale per le Pubbliche Amministrazioni in armonia con i lavori della *European Blockchain Systems Infrastructure*, quale pilastro della strategia europea *Connected Europe Facility*.

³⁸ Si veda, al riguardo, la Risoluzione del Parlamento europeo del 3 ottobre 2018 sulle tecnologie di registro distribuito e *blockchain*: creare fiducia attraverso la disintermediazione (2017/2772(RSP)), sulla quale più diffusamente *infra*.

³⁹ Nella consultazione pubblica avviata nel giugno 2020 sulla Strategia nazionale per *blockchain* e registri distribuiti, infatti, il MISE ha pubblicato un documento – redatto dal gruppo di esperti – contenente delle linee guida con raccomandazioni generiche ed indeterminate, specie sotto il profilo giuridico-regolatorio. Cfr. sul punto <https://www.mise.gov.it/index.php/it/consultazione-blockchain>.

⁴⁰ La *blockchain* inizia a trovare largo uso tra gli operatori di mercato maggiormente sensibili all’innovazione tecnologica. Sulle diverse applicazioni pratico-operative di una simile tecnologia, senza alcuna pretesa di esaustività, si rinvia ai diversi approfondimenti tematici contenuti in R. Battaglini, M.T. Giordano (a cura di), *Blockchain e Smart Contract. Funzionamento, profili giuridici e internazionali, applicazioni pratiche*, Milano, 2019.

Ad ogni modo, al di là di ogni considerazione di natura tecnica sull'effettiva valenza "certificativa" delle transazioni e di riduzione delle inefficienze e semplificazione dei livelli di intermediazione, occorre rilevare come, a tutt'oggi, e in modo disarmante, la *blockchain* sia una tecnologia priva di qualsiasi meccanismo di controllo, organismo di vigilanza e, quindi, di responsabilità e "rendicontazione" del proprio operato. Il registro digitale, infatti, segue delle logiche informatiche di funzionamento che sono rimesse ai criteri più o meno strutturati della sua programmazione e, proprio perché distribuito, non è archiviato centralmente da nessuno, perché tutti gli attori coinvolti nell'infrastruttura informatica ne mantengono una copia simultanea. Ma se tutti sono responsabili della corretta tenuta del registro, nessuno sarà mai effettivamente responsabile di eventuali abusi (e anche ove fosse, a che titolo?), perché non esiste alcun ordine gerarchico all'interno delle piattaforme tecnologiche basate sui registri distribuiti, definite per l'appunto *peer to peer*, potendo gli operatori agire solo previo "consenso"⁴¹ della maggioranza, il più delle volte anonima⁴² e "polverizzata" in chissà quale parte del globo.

Come evidenziato sul punto dalla Risoluzione del Parlamento europeo del 3 ottobre 2018⁴³, inoltre, i rischi e i problemi della tecnologia non sono ancora completamente noti, e i problemi e le preoccupazioni connessi all'applicazione di regolamentazioni e norme orizzontali, riguardanti questioni come la protezione dei dati o l'imposizione fiscale, possono inibirne il potenziale di sviluppo tecnologico. Analogo approccio è stato poi seguito anche dalla Commissione Europea, nel suo *Study on Blockchains - Legal, governance and interoperability aspects (SMART 2018/0038)*⁴⁴ del 28 febbraio 2020, laddove rileva come, tra le problematiche giuridiche relative alla *blockchain*, vi siano delle barriere rappresentate dalla legislazione settoriale, che potrebbe "impedire" il pieno sfruttamento delle potenzialità tecnologiche e la protezione dei principi giuridici fondamentali e delle norme dell'Unione Europea, primi fra tutti la protezione dei dati⁴⁵.

⁴¹ Sul punto, oltre a quanto già argomentato *supra*, par. 2 *sub* nota 14, cfr. più diffusamente *infra*, par. 6.

⁴² A differenza del sistema previsto dal Codice dell'Amministrazione digitale e del regolamento eIDAS, in materia di firma digitale, dove sussiste un processo preliminare di identificazione che consente di avere l'effettiva certezza dell'identità del titolare della coppia di chiavi, nel sistema ad esempio della *bitcoin blockchain* infatti, anch'esso di tipo asimmetrico o a chiave pubblica, chiunque può ottenere una coppia di chiavi, privata e pubblica, per scambiare criptovaluta senza la necessità di doversi preventivamente identificare.

⁴³ Risoluzione sulle tecnologie di registro distribuito e *blockchain*: creare fiducia attraverso la disintermediazione (2017/2772(RSP)).

⁴⁴ Accessibile al sito <https://ec.europa.eu/digital-single-market/en/news/study-blockchains-legal-governance-and-interoperability-aspects-smart-20180038>.

⁴⁵ Si vedano, al riguardo, A.L. Seretakis, *Blockchain, Securities Markets, and Central Banking*, in P. Hacker, I. Lianos, G. Dimitropoulos, S. Eich (a cura di), *Regulating Blockchain: Techno-Social and Legal Challenges*, Oxford, 2019, 224.

Nello specifico, appare opportuno evidenziare che, rispetto al tema della protezione dei dati e dell'eventuale difficoltà a garantire il diritto all'oblio⁴⁶, un primo profilo problematico della tecnologia, non di poco conto, e che appare giuridicamente rilevante, è rappresentato dal rischio di c.d. collisione delle funzioni crittografiche di *hash*⁴⁷, il quale, potendo astrattamente generare la stessa stringa alfanumerica di uscita da due documenti diversi, mina alla radice la presunzione di affidabilità incondizionata della matematica sul diritto e, con tutte le riserve sulle potenziali contaminazioni meta-giuridiche⁴⁸, non è stato ancora scandagliato a dovere dalla letteratura giuridica.

Un secondo profilo problematico, è dato dalle zone d'ombra di scarsa tracciabilità delle operazioni registrate sulla *blockchain*, specie quella pura, cioè *permissionless* nel senso di "pubblica" laddove nessuno identifica le parti chiamate a operare sul registro e sui nodi, che possono geo-localizzarsi ovunque, con tutto ciò che ne consegue in termini di repressione di abusi informatici. La *blockchain*, pertanto, specie quella pubblica, cioè aperta con l'insieme di nodi decentralizzati ma interconnessi, vive in uno spazio di sostanziale vuoto normativo, come se fosse una flotta senza bandiera in un *Mare liberum* digitale.

Il terzo problema, prettamente giuridico, connesso alla *blockchain*, tale da rappresentare forse il vero nodo gordiano dell'analisi qui proposta, è dato dalla difficile ipotizzabilità di risolvere il problema delle asimmetrie informative e della mancanza di fiducia in assenza di intermediari affidabili e centralizzati.

Sul piano prettamente giuridico, infatti, prescindendo anche dalla eventuale adozione o meno delle linee guida dell'AgID, la prima domanda da porsi attiene a quale valore attribuire alla "certificazione" informatica offerta dalle *blockchain*. Riprendendo la scelta legislativa offerta dal d.l. 135/2018, gli effetti giuridici pro-

⁴⁶ La necessaria economia del presente contributo non consente una trattazione approfondita sui potenziali risvolti problematici legati al tema della protezione dati, per il quale si rinvia, *ex multis*, a A.M. Gambino, C. Bomprezzi, *Blockchain e Protezione dei Dati Personali*, in *Dir. inf. e inform.*, 2019, 3, 655. Sul panorama della letteratura giuridica comparata si vedano M. Berberich, M. Steiner, *Blockchain Technology and the GDPR. How to Reconcile Privacy and Distributed Ledgers?*, in *European Data Protection Law Review*, 2, 2016, 422; e da ultimo L. Moerel, *Blockchain & Data Protection... and Why They Are Not on a Collision Course*, in *European Review of Private Law*, 2019, 6, 825. Sul versante istituzionale, occorre segnalare come nell'ordinamento francese, la *Commission nationale de l'informatique et des libertés* ha prodotto nel settembre 2018 il rapporto *Blockchain et RGPD: Quelle solution pour un usage responsable en présence de données personnelles?* con il quale ha evidenziato dubbi e criticità operative sull'esercizio del diritto alla cancellazione dei dati personali.

⁴⁷ Non è questa la sede per approfondire la questione, comunque centrale, dei rischi matematici di collisione delle funzioni di *hash*. Senza alcuna pretesa di esaustività sul tema, si rinvia per le collisioni di *hash* a M. Stevens, E. Bursztein, P. Karpman, A. Albertini, Y. Markov, *The first collision for full SHA-1*, 2017, 570 s.; P. Karpman, T. Peyrin, M. Stevens, *Practical free-start collision attacks on 76-step SHA-1*, 2015, 663.

⁴⁸ Ai fini dell'analisi giuridica, infatti, sarà necessario evidenziarne il problema, giuridicamente rilevante, senza intorbidire il ragionamento con contaminazioni inter-disciplinari estranee al diritto, e vale sempre la pena di richiamare le parole di Carnelutti, mai cattivo Maestro, secondo il quale «a risolvere i problemi giuridici, è sufficiente la logica di un ignorante», in *Studio sulle energie come oggetto di rapporti giuridici*, in *Riv. dir. comm.*, 1913, 354 s.

dotti dalle tecnologie basate su registri distribuiti sono gli stessi della validazione temporale elettronica di cui all'articolo 41 del regolamento (UE) n. 910/2014, e cioè: 1. non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziari; 2. godono della "presunzione di accuratezza" della data e dell'ora che indicano e di integrità dei dati ai quali tale data e ora sono associate.

Ma nel merito, chi è che assicura che i dati riportati e trascritti nel registro, siano corretti e veritieri, cioè che siano "certi"? Detto altrimenti, chi ha la responsabilità di fornire "certezza" sul contenuto dei dati trascritti? E chi ha interesse al *proof of work* e alla validazione delle relative transazioni?

Appare quindi necessario investigare se sia possibile fornire di certezza giuridica i fatti giuridicamente rilevanti da trascrivere nella *blockchain*, intesi nel senso proprio di fatti produttivi di effetti giuridici. Detto in altri termini, è necessario investigare se la tecnologia offra dei margini di manovra per avvolgere di "verità fattuale" giuridicamente rilevante il dato trascritto.

La questione giuridica aperta non è certo di poco conto, atteso che, dal punto di vista meramente estrinseco, i dati inseriti, una volta trascritti nel registro distribuito, ben possono rientrare nella nozione di "documento informatico" offerta dal Codice dell'Amministrazione Digitale, il quale all'art. 1, comma, 1, lett. p), lo definisce come la «rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti», o anche alla stregua di un "documento elettronico", definito come «qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva».

Se questa assimilazione appare quasi del tutto lineare e coerente con la libertà ordinamentale riconosciuta alle forme, ancorché digitali, appare però molto più spinosa la questione sull'effettiva riconducibilità delle dichiarazioni e informazioni di un nodo della *blockchain* al soggetto che lo ha generato⁴⁹, specie in assenza di un intermediario fidefaciente⁵⁰.

In questo senso, assume un'attuale rilevanza l'insegnamento di Giannini sui procedimenti dichiarativi, i quali «in quanto volti a dare certezza ai fatti, constano sempre di due momenti logici: uno di acquisizione, l'altro di dichiarazione»⁵¹. Il primo momento rappresenta l'acquisizione materiale del fatto, descrivendo

⁴⁹ Cfr. M. Giuliano, *op. cit.*

⁵⁰ Si veda, in tal senso, il privilegio riconosciuto dall'art. 23-ter del CAD proprio ai "Documenti amministrativi informatici", ai sensi del quale «Gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi o identici tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge»; nonché la previsione del successivo comma 1-bis, per il quale «La copia su supporto informatico di documenti formati dalle pubbliche amministrazioni in origine su supporto analogico è prodotta mediante processi e strumenti che assicurano che il documento informatico abbia contenuto identico a quello del documento analogico da cui è tratto, previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza del contenuto dell'originale e della copia».

⁵¹ M.S. Giannini, *Diritto Amministrativo*, II, Milano, 1970, 954.

in che cosa questo consiste. Nel secondo, quello certificativo vero e proprio, si dichiara verso l'esterno ciò che è stato acquisito⁵².

Ma il funzionamento decentralizzato della *blockchain*, espone inevitabilmente il fianco all'interrogativo di fondo sul "se" sia possibile davvero trasformare i meccanismi classici di fiducia sulla qualità delle informazioni trascritte, vicariando ai privati, senza regole e senza controlli, la relativa funzione certificativa in formato digitale. Detto altrimenti: a chi si imputano gli atti formati nella *blockchain*?

5. *Pubblico e privato nell'attività di certificazione: l'aporia cripto-anarchica dell'informatica*

Il presupposto ideologico delle tecnologie basate sui registri distribuiti, come è noto, risiede nella condivisione totalizzante di un unico registro madre, nell'intento di sopperire alla mancanza di fiducia nei riguardi di un unico intermediario centrale.

Questa sfiducia generalizzata verso gli intermediari, e verso le preposte istituzioni di vigilanza, come è altrettanto noto, è stata ancor più sentita all'indomani della crisi economica del 2008, e non è certo un caso che lo sviluppo iniziale della *blockchain*, sempre del 2008, si ponga in linea di continuità e concomitanza temporale con la crisi di fiducia generata dalla bolla dei mutui *subprime*⁵³.

In questo contesto, infatti, il prodromo delle tecnologie basate sui registri distribuiti è stata proprio la *bitcoin blockchain*, che ha registrato la prima transazione il 3 gennaio 2009 e il funzionamento crittografico della quale (*i.e.* unicità del valore digitale ed eliminazione del *double spending*) ha rappresentato il "libro mastro" che ha permesso la trascrizione degli scambi delle criptovalute, erroneamente intese come "moneta" e per di più alternativa alle tradizionali divise di Stato⁵⁴.

⁵² Sugli indirizzi della scienza moderna, circa la certezza e la verità, si vedano principalmente: M.S. Giannini, *Certezza pubblica*, cit.; nonché Id. e A. Falzea, *Accertamento (teoria generale)*, in *Enc. dir.*, vol. I, Milano, 1958; A. Stoppani, *Certificazione*, in *Enc. dir.*, vol. VI, Milano 1960. Cfr. S. Pugliatti, *La trascrizione*, Milano, 1957; nonché C. Vitta, *Gli atti certificativi e le decisioni amministrative*, in *Giur. it.*, 1924, IV, 125.

⁵³ L'economia di questo contributo non consente un'approfondita trattazione sulle origini e sugli effetti della crisi dei mutui *sub-prime*. Per una descrizione delle diverse cause si rinvia *ex multis* ai rilievi di J.E. Stiglitz, *Macroeconomics, Monetary Policy and the Crisis*, in O. Blanchard, D. Romer, M. Soence, L.E. Stiglitz (eds.), *In the Wake of the Crisis*, Cambridge, 2013; K. Rogoff, Reinhart, M. Carmen, *Financial and Sovereign Debt Crises: Some Lessons Learned and Those Forgotten*, in S. Claessens, M.A. Kose, L. Laeven, F. Valencia (eds.), *Financial Crises: Causes, Consequences, and Policy Responses*. Presented September 14, 2012, at IMF conference on financial crises, Washington, DC, 2014. Per la dottrina italiana, si vedano *ex multis* N. Salanitro, *Capitalizzazione e crisi economica*, in *Banca, borsa e titoli di credito*, 2010, 125 s., e M. Onado, *La crisi finanziaria internazionale: le lezioni per i regolatori*, in *Banca, impresa e società*, 2009, 5 s.

⁵⁴ Per analoghe ragioni di economia del presente contributo, non è possibile una trattazione in questa sede della natura giuridica delle criptovalute e dei problemi giuridico-regolatori da esse sollevati. Sul punto, sia

Secondo l'ideologia cripto-anarchica, pertanto, l'utilizzo delle funzioni crittografiche di *hash*, unite alla distribuzione del registro digitale, avrebbe consentito – e in parte così è stato, almeno per la *bitcoin blockchain* – la diffusione di valori digitali “certi” senza l'ausilio di alcun intermediario centralizzato, laddove l'idea stessa di necessarietà di una simile figura istituzionale era stata del tutto delegittimata a seguito della nota vicenda del *rating* falsato riconosciuto alla *Lehman Brothers* nell'imminenza del suo fallimento.

Il presupposto operativo di tale ideologia, tuttavia, si fonda sull'interesse dei *miners*, a mettere a disposizione la propria capacità computazionale per validare il blocco da trascrivere, e questa operazione “pubblica” – nel senso di collettiva – sarebbe la garanzia di trasparenza e di effettiva “certezza” richiesta per ritenere il sistema affidabile.

Ma questa asserita funzione certificativa che dovrebbe essere demandata ai *miners*, non consente in alcun modo di intorbidire il ragionamento giuridico rispolverando la teoria dell'esercizio privato delle pubbliche funzioni⁵⁵ – nel caso di specie, di certificazione – laddove un'eventuale traslazione *sic et simpliciter* alle tecnologie basate sui registri distribuiti, oltre a rievocare tutte le note problematiche dottrinarie di una simile ricostruzione⁵⁶, si scontra con due preclusioni obiettive, una formale, l'altra sostanziale.

consentito un rinvio al mio *Contributo allo studio sulle criptovalute come oggetto di rapporti giuridici*, cit., e alla bibliografia di autori ivi citata.

⁵⁵ La categoria dell'esercizio privato delle pubbliche funzioni, come è noto, è stata introdotta da Santi Romano, nel suo *Principii di diritto amministrativo*, Milano, 1912, 189 s. Zanobini ha poi provveduto ad un'elaborazione sistematica della stessa nozione, secondo la quale questa ricomprende qualunque opera di esplicazione di una potestà propria dello stato o di altro ente pubblico, vicariata ai privati che non rivestano alcuna qualifica o qualità di organo di tali enti. Sostanzialmente, due sono gli elementi essenziali della figura: la pubblicità della funzione e la natura privatistica del soggetto che la esercita. Sul punto, si rinvia a G. Zanobini, *L'esercizio privato delle funzioni e dei servizi pubblici*, in V.E. Orlando (a cura di), *Trattato di Diritto Amministrativo Italiano*, II, Società Editrice Libreria, Milano, 1920; nonché, per una rielaborazione moderna, ad A. Maltoni, *Esercizio privato di pubbliche funzioni*, in *Enc. dir.*, Annali, I, Milano, 2007; G. Napolitano, *L'esercizio privato di attività amministrative*, in V. Cerulli Irelli (a cura di), *La disciplina generale dell'azione amministrativa*, Napoli, 2006; nonché, da ultimo, A. Benedetti, *Certezza pubblica e “certezze” private. Poteri pubblici e certificazioni di mercato*, Milano, 2010, spec. 17, cui si rinvia per ulteriori riferimenti dottrinari sulla contrapposizione pubblico-privata nelle certificazioni.

⁵⁶ Appare infatti necessario specificare e distinguere la categoria dei privati che pongono in essere tale attività per un proprio interesse, da coloro che svolgono in assenza dello stesso. Tuttavia, come già rilevato da Nigro, infatti, la nozione di esercizio privato di pubbliche funzioni è stata elaborata per sistemare unitariamente alcuni fenomeni, diversissimi fra loro, ma tutti egualmente caratterizzati dal fatto di non essere riconducibili – “imputabili” – all'organizzazione amministrativa nella sua struttura propria. Poiché di questa organizzazione amministrativa si aveva una nozione molto ristretta ed elementare, conforme del testo allo sviluppo dell'organizzazione stessa in quel momento, la nozione apparve idonea a spiegare non solo i casi di occasionale esercizio di un'attività pubblica da parte di un privato, ma anche quegli altri in cui, pur essendo l'esercizio più stabile e continuativo, non di riusciva a reperire alcuna persona giuridica a cui riferirlo, oppure, quantomeno, il nesso di riferimento appariva largo e anomalo. Cfr. sul punto M. Nigro, *Il notaio nel diritto pubblico*, in *Riv. trim. dir. pubbl.*, 1979, 441, il quale rileva altresì la sintomaticità del fatto che Zanobini, dopo aver distinto l'organizzazione amministrativa in organizzazione dello Stato e organizzazione degli enti autarchici, una volta passato a

Sulla preclusione di tipo formale, varrebbe la considerazione per la quale, al momento, non c'è stata alcuna attribuzione legislativa che abbia demandato ai *miners* la titolarità giuridica di alcun *munus* pubblico, sia in proprio sia delegato⁵⁷ (anzi, il loro presupposto è proprio l'assenza di qualsiasi legittimazione⁵⁸) così come la relativa attività non riveste alcun carattere di doverosità o di procedimentalizzazione. Né, al contempo, le altre esperienze pratico-operative recenti, in cui le funzioni certificative sono state direttamente vicariate ai privati, ovvero che non trovano addirittura la loro legittimazione primigenia dall'ordinamento statale, potrebbero fungere da "precedente" per ampliare il novero delle certificazioni volontaristiche di mercato (si pensi alle valutazioni delle agenzie di *rating*, alle attestazioni SOA, alle certificazioni ISO o ai marchi DOP-IGP). Queste, infatti, hanno visto l'attribuzione a dei soggetti terzi – esterni sì al perimetro pubblicistico, ma almeno operanti in concorrenza tra loro in dei mercati regolamentati – essere stata comunque temperata o dalla preventiva qualificazione e accreditamento⁵⁹ dei certificatori o comunque dalla previsione di poteri di vigilanza e sanzionatori in caso di loro abusi⁶⁰.

trattare dell'esercizio privato, avvertisse che «l'esercizio privato non rappresenta [...] una terza specie di amministrazione, dopo quella dello Stato e degli enti autarchici: si tratta, invece, di un mezzo particolare, e diverso da quelli fin qui esaminati, di cui di valgono tanto lo Stato quanto gli enti anzidetti». La teoria dell'esercizio privato di pubbliche funzioni, come è noto, aveva suscitato un vivace dibattito tra i Maestri del diritto amministrativo, sintetizzabile nelle evidenziate posizioni di Zanolini, sulla teoria dell'organo indiretto, e in quelle di Giannini, sulla nozione di *munus*, le quali basavano il quadro prospettico dell'indagine sulla solidità dell'impianto concettuale, che teorizzava l'esercizio di poteri pubblici da parte di soggetti non appartenenti all'apparato pubblico, senza per questo minare l'unitarietà della costruzione pubblicistica Stato-centrica che vedeva nello Stato, espressione massima del potere sovrano, l'accentratore della funzione pubblicistica di produzione della certezza legale. Sul punto, si rinvia ad A. Benedetti, *Certificazioni "private" e pubblica fiducia*, in *Dir. econ.*, 2006, 1, spec. 11.

⁵⁷ Come è noto, la titolarità o meno della potestà rileva sul piano giuridico, laddove se è l'Amministrazione a conferire al privato l'esercizio della funzione, la stessa ne rimane titolare esclusiva, conserva poteri di indirizzo, di controllo e di revoca; mentre invece laddove il privato riceve l'investitura della funzione direttamente dalla legge, permane nell'ordinamento il potere di vigilanza e controllo in capo ad un'autorità pubblica.

⁵⁸ Vale la pena richiamare A. Stoppani, op. cit., laddove rileva che «È, in ogni caso, necessario mettere in luce una prospettiva fondamentale comune a tutti i privati investiti di *munera* pubblici; l'attività ch'essi pongono in essere costituisce sempre una certezza pubblica, con tutte le conseguenze che ne scaturiscono».

⁵⁹ Si pensi, ad esempio, al sistema di registrazione previsto per le agenzie di *rating* così come previsto dal Regolamento CE n. 1060/2009 in materia di riconoscimento delle Agenzie di *rating* Europee sottoposte alla vigilanza dell'*European Securities and Markets Authority* (ESMA).

⁶⁰ Sul punto, cfr. i rilievi di A. Benedetti, *Le agenzie di rating tra crisi dei modelli di mercato e criticità dei processi di regolamentazione*, in *www.costituzionalismo.it*, 2012, 2, 21 s.; G. La Rosa, *Il ruolo delle agenzie di rating*, in *Dir. econ.*, 2012, 1, 25 s.; L. Pianesi, *Le agenzie di rating tra privatizzazione di funzioni pubbliche e opinioni private "geneticamente modificate"*, in *Riv. trim. dir. pubbl.*, 2011, 179 ss. Sulla critica al *rating* quale strumento di controllo del rischio a oligopolio privato, cfr. M. Passalacqua, *Diritto del rischio nei mercati finanziari: prevenzione, precauzione ed emergenza*, Padova, 2012, spec. 156, nonché G. Ferri, P. Lacitignola, *Concorrenza e agenzie di "rating": il dibattito economico*, in *Analisi giur. econ.*, 2012, 2, 299 s. Per una riflessione più approfondita sulle dubbie implicazioni dell'attività valutativa delle agenzie di *rating* si rinvia ad A. Benedetti, *Certezza pubblica e "certezze" private*, cit.; G. Ferri, P. Lacitignola, *Le agenzie di rating*, Bologna, 2009, nonché C. Pinelli, *L'incontrollato potere delle agenzie di rating*, in *www.costituzionalismo.it*, 2012, 1.

Come è stato già osservato in dottrina, infatti, la funzionalità del sistema delle certificazioni privatistiche si fonderebbe in realtà su dei meccanismi di mercato di “credibilità” e di “autorevolezza” di chi certifica (oltre che di chi controlla i certificatori), ancor più nelle ipotesi di certificazioni puramente volontarie richieste dagli operatori unicamente per guadagnare appetibilità commerciale e quote di mercato⁶¹.

Ad analoghe considerazioni, ugualmente escludenti, deve giungersi con riferimento all’ipotesi più prossima delle certificazioni di firma digitale, volte a garantire l’affidamento pubblicistico sull’imputazione soggettiva e l’identificazione puntuale della titolarità delle firme. Sebbene, infatti, i certificatori di firma digitale condividano con la *blockchain* un sistema crittografico di coppie di chiavi asimmetriche – una pubblica e una privata – l’attività di certificazione in questa ipotesi ha come unico effetto la non disconoscibilità del documento sottoscritto e l’identificazione precisa del sottoscrittore digitale, laddove il vero *punctum dolens* della *blockchain*, nell’interpretazione qui proposta, non è rappresentato tanto dalla soggettività dell’imputazione legale di chi fornisce il dato (come invece è nella firma digitale, e che comunque rappresenta allo stato un problema innegabile di identificazione e tracciabilità degli operatori della *blockchain*), quanto dalla garanzia di genuinità delle informazioni trascritte.

Venendo alla preclusione di tipo sostanziale, bisogna riconoscere come, notoriamente, il soggetto privato chiamato a cooperare in attività di interesse generale, sia disponibile a prestare la propria attività solo allorquando vi corrisponda un proprio interesse personale, di base imperniato su impulsi di tipo egoistico e lucrativo⁶². Questo paradigma è ancor più evidente laddove si consideri che, nell’unico precedente di diffusione veramente globale di tecnologia basata su registri distribuiti, la *bitcoin blockchain*, il sistema ha funzionato – e continua a funzionare – proprio perché i *miners* ottengono dei *bitcoin* come premio per la validazione dei nodi.

⁶¹ Il riferimento è all’elaborazione scientifica di A. Benedetti, *Certificazioni “private” e pubblica fiducia*, cit., spec. 16, laddove rileva che «Dovendosi necessariamente schematizzare le caratteristiche di questi sistemi di certificazione privata, si può affermare che essi rappresentano forme di istituzionalizzazione della fiducia collettiva che non traggono la propria legittimazione dagli ordinamenti giuridici nazionali o sovranazionali. In essi, infatti: la “struttura istituzionale” è rappresentata da reti internazionali di organismi di natura privatistica, che traggono la propria legittimazione da forme di partecipazione reciproca e da accordi di mutuo riconoscimento: così è per gli enti di normazione (deputati alla formulazione delle norme tecniche), nazionali e internazionali, che sono organizzati in forma di associazioni privatistiche (partecipate dalle istanze del mondo produttivo e da soggetti pubblici, che non assumono tuttavia una posizione di controllo); così è anche per gli enti di accreditamento, creati per “abilitare” e controllare i soggetti privati certificatori; i certificatori sono imprese private, che operano in concorrenza sul mercato e la cui attività si esplica nella verifica dell’oggetto (prodotto, processo produttivo, organizzazione) rispetto alle norme tecniche di riferimento, mediante la formulazione di giudizi tecnici e sulla base di un contratto stipulato con l’impresa (o l’organizzazione) interessata alla certificazione».

⁶² Cfr. sul punto, M.S. Giannini, *Esercizio privato di pubbliche attività*, in *Enc. dir.*, vol. XV, Milano, 1966, 685 s., A. Azzena, *Esercizio privato di pubbliche funzioni e di pubblici servizi*, in *Dig. disc. pubbl.*, vol. VI, Torino, 1991, 165 s., nonché, da ultimo, A. Maltoni, *Il conferimento di potestà pubbliche ai privati*, Torino, 2005, a cui si rinvia per ulteriori riferimenti bibliografici.

Questa considerazione, in ultima analisi, impone un'attenta riflessione sui meccanismi di consenso che sono alla base dei sistemi di validazione della *blockchain*, laddove la potenziale componente di natura patrimoniale sottesa all'interesse dei *miners* appare poco conciliabile con un mandato pubblicistico di verifica della qualità dell'informazione. Infatti, atteso che anche i normali certificatori "di mercato" ottengono una remunerazione per l'attività svolta, al pari degli stessi notai – certificatori pubblici per eccellenza – occorre però evidenziare che, nell'asserito circuito certificativo dei *miners*, permane l'assenza di qualsiasi paracadute deontologico e di vigilanza istituzionale idoneo a impedire comportamenti scorretti, ovvero in palese conflitto di interessi rispetto alla *res* da certificare.

L'imbarazzo è ancor più evidente se si considera l'inversione terminologica della dicotomia pubblico-privato applicata alla *blockchain* nei linguaggi giuridico e tecnico. Nella terminologia informatica, infatti, la *blockchain* "pubblica" non è sinonimo di statale, ma di collettiva e senza restrizioni (*permissionless*), e *blockchain* "privata" non significa al di fuori del perimetro pubblico, ma solamente nel senso di ristretta, controllata (*permissioned*).

Il problema non è solo di tipo linguistico (*nomina sunt consequentia rerum*) atteso che tutte le *blockchain*, per funzionare, hanno bisogno del "consenso", cioè che i *miners* raggiungano un accordo sul "set" di informazioni da trascrivere. E questo consenso viene raggiunto ricorrendo a un algoritmo per confermare le transazioni e produrre i nuovi blocchi della catena.

Questa "delega di funzioni" all'algoritmo, in ultima analisi, rappresenterebbe la chiave di volta che mantiene la struttura fiduciaria riposta nei riguardi di una simile tecnologia. Ed è proprio questo il *locus commissi delicti* dove si consuma l'aporia cripto-anarchica.

L'aver predisposto un'infrastruttura crittografica "autoportante" di transazioni digitali, infatti, avrebbe voluto sovvertire e risolvere "in house" la crisi di fiducia delle istituzioni di intermediazione attraverso l'intervento di protocolli informatici decentralizzati e distribuiti che, dalla prospettiva puramente matematica, godono di un livello di certezza pressoché totale.

Tuttavia, allo stato attuale, sussistono non poche perplessità sulla tenuta delle funzioni crittografiche di *hash* dal rischio di collisione⁶³, fattore che spie-

⁶³ In questa sede, è sufficiente limitarsi a segnalare il problema della collisione, che è stato affrontato e dibattuto nel linguaggio che è proprio di altre discipline non-giuridiche, per le quali si rinvia ad A. Viola, *Exact-distribution of individual displacements in linear probing hashing*. *Transactions on Algorithms* (TALG), October 2005, 1 (2), 214 s.; M. Herlihy, N. Shavit, M. Tzafrir, "Hopscotch Hashing". *DISC '08: Proceedings of the 22nd international symposium on Distributed Computing*, Berlin-Heidelberg, 2008, 350 s.; T. Cormen, C. Leiserson, R. Rivest, Stein, *Chapter 11: Hash Tables*. *Introduction to Algorithms* (2nd ed.), Clifford, 2001, 221 s.; N. Askitis, J. Zobel, *Cache-conscious Collision Resolution in String Hash Tables*. *Proceedings of the 12th International Conference, String Processing and Information Retrieval* (SPIRE 2005), October 2005, 3772/2005, 91 s.; N. Askitis, R. Sinha, *Engineering scalable, cache and space efficient tries for strings*, in *The VLDB Journal*, 2010, 17 (5),

ga i propri effetti in ambito giuridico laddove la “sicurezza” del processo crittografico alla base dell’intera struttura non è affatto immune da pericolose zone d’ombra e cortocircuiti. Inoltre, quello che i cripto-anarchici non considerano nel loro intento de-regolamentatorio delle transazioni, oltretutto predisposto con un sistema slegato da qualsiasi ordinamento giuridico di matrice statale, è che la crisi del 2008, tra le diverse concause, è derivata proprio da una miope de-regolamentazione dell’attività bancaria e della vigilanza ad essa prudenziale⁶⁴.

Verrebbe da chiedersi, pertanto, quanto possa effettivamente consolidarsi e diffondersi un sistema che permette lo scambio digitale di beni in una comunità ristretta di esperti informatici⁶⁵, senza intermediari, senza regole, con dei buchi di programmazione dovuti ai limiti e alla fallacia dei numeri⁶⁶ e con un meccanismo di “consenso” tutt’altro che cristallino.

6. *La notarizzazione impossibile: il problema dei generali bizantini tra consenso, accertamenti fattuali e potestà pubblicistiche*

Un profilo di criticità ulteriore, che emerge in seno all’indagine sui profili giuridici della *blockchain*, attiene ai risvolti problematici derivanti da un’ipotetica funzione di notarizzazione dei dati.

Come già evidenziato, infatti, la funzione primaria delle tecnologie basate sui registri distribuiti è quella di “certificare” le avvenute transazioni, garan-

633 s.; N. Askitis, *Fast and Compact Hash Tables for Integer Keys*. Proceedings of the 32nd Australasian Computer Science Conference (ACSC 2009), 91, 113 s.

⁶⁴ Come è noto, durante l’amministrazione Clinton, con l’emanazione dal *Gramm-Leach-Bliley Act* del 1999 sono state abrogate le disposizioni del *Glass-Steagall Act* del 1933 sulla separazione tra attività bancaria tradizionale e attività d’investimento e le disposizioni del *Bank Holding Company Act* del 1956 sul divieto per le banche commerciali di svolgere attività assicurativa. La sregolata despecializzazione delle attività e gli scarsi e inefficaci controlli delle autorità di vigilanza hanno segnato la crisi lenta e profonda in termini di solvibilità patrimoniale. Nell’economia del presente lavoro, sul punto si veda F. Capriglione, *Concentrazioni bancarie e logica di mercato*. Relazione al Seminario di studi su “Concentrazioni bancarie e tutela della concorrenza dopo l’entrata in vigore della legge sul risparmio: considerazioni teoriche e problemi applicativi”, Pisa, 19 maggio 2007, in *Banca, borsa e titoli di credito*, 3, 2008, 293 ss., nonché sia consentito richiamare il mio *L’evoluzione pubblicistica del “governo delle banche” tra Stato e mercato*, in *P.A. Persona e Amministrazione*, 2018, 2, 431 s.

⁶⁵ Anche la scienza economica inizia a manifestare un approccio critico e dubitativo sulle tecnologie basate sui registri distribuiti, non riuscendo queste a sviluppare dei protocolli informatici di base comuni e universali che rendessero il dietro le quinte di *internet* disponibile al pubblico, il che, traslato nel contesto della *blockchain*, renderebbe la promessa di transazioni decentralizzate senza intermediari un “sogno utopico e dubbio”. Cfr. sul punto N. Roubini, *Broken Promises of the Blockchain*, in *Project Syndicate*, <https://www.project-syndicate.org/commentary/why-bitcoin-is-a-bubble-by-nouriel-roubini-2018-01?barrier=accesspaylog>.

⁶⁶ Si cfr. sul punto gli scritti intorno ai principi di incompletezza e di indecidibilità dei sistemi matematici di D. Lindley, *Incertezza. Einstein, Heisenberg, Bohr e il principio di indeterminazione*, Einaudi, 2008; W. Heisenberg, *Indeterminazione e realtà*, Napoli, 2002; G. Gigerenzer, *Quando i numeri ingannano. Imparare a vivere con l’incertezza*, Milano, 2003, nonché H. Bandemer, *Mathematics of Uncertainty. Ideas, Methods, Application Problems*, Berlin-Heidelberg, 2006.

tendo l'immutabilità e l'imputazione cronologica della menzionata "impronta digitale"⁶⁷ riconosciuta al file trascritto, tra un passaggio di mano e l'altro.

Attraverso la notarizzazione informatica, pertanto, si vorrebbe garantire la conformità del file originale e la relativa "data certa", ritenendo però – in grave errore – di poter disporre anche di un fatto giuridicamente rilevante, vincolante e, per ciò solo, "immutabile".

Ma l'architettura informatica della *blockchain*, proprio perché presuppone l'assenza di un'autorità centrale, determina la necessità di ottenere il "consenso" dei vari validatori sull'esattezza dello stato di avanzamento della catena tra un anello e l'altro.

Nello specifico, la ricerca del consenso tra gli operatori si sostanzia in un processo informatico di raggiungimento di un "accordo decisionale" su ciascuno stato di avanzamento, tale da escludere dubbi o incertezze sul singolo anello e cristallizzare la "verità" della situazione dello stato attuale.

Tuttavia, il problema di base della *blockchain* – ancor più se *permissionless* – è rappresentato proprio dalla necessità di raggiungere il consenso, in assenza di gerarchie e di vigilanza, tra degli operatori che non si conoscono, ma che devono interagire e accordarsi sulle soluzioni da adottare ed evitare possibili comportamenti di natura predatoria o scorretta.

La complessità dell'ottenimento del consenso nell'ambito delle tecnologie basate sui registri distribuiti, impone, perciò, la ricerca di strumenti diretti a superare i problemi di fiducia nello scambio di informazioni del sistema dei voti e dei consensi dei nodi; in questo contesto le strade seguite dalla prassi informatica hanno visto due approcci diversi; il raggiungimento del consenso per il tramite del menzionato *proof of work*, e il c.d. *Byzantine Fault Tolerance* come soluzione del noto problema dei generali bizantini⁶⁸, quando cioè più parti devono prendere simultaneamente la stessa decisione in presenza di possibili errori e di informazioni discordanti, potendo comunicare solo tramite messaggi. L'esperienza pratica finora maggiormente adottata – parliamo della *bitcoin blockchain* – ha visto l'adozione di un algoritmo di consenso volto alla risoluzione del problema, laddove ha obbligato i *miners*, per validare il blocco da aggiungere, a competere l'u-

⁶⁷ Si vedano, al riguardo, le argomentazioni riportate *supra*, par. 2.

⁶⁸ Il problema dei generali bizantini, come è noto, richiede di risolvere l'incertezza che si genera tra un gruppo di generali, ciascuno al comando di una porzione dell'esercito bizantino durante un assedio, laddove questi devono decidere simultaneamente se attaccare o ritirarsi. Ciò che rileva, al netto della strategia offensiva o difensiva prescelta, è il raggiungimento del consenso unanime affinché vi sia un coordinamento strategico tra le varie unità, evitando il rischio che dei generali disonesti possano fornire informazioni fuorvianti ovvero comunicare le proprie intenzioni solo ad alcuni. Sul punto, senza alcuna pretesa di completezza, si rinvia per gli opportuni approfondimenti metodologici di risoluzione a L. Lamport, R. Shostak, M. Pease, *The Byzantine Generals Problem*, in *ACM Transactions on Programming Languages and Systems*, luglio 1982, vol. 4 (3), 382.

no con l'altro nella risoluzione di un problema matematico⁶⁹, ricercando per tentativi un "determinato"⁷⁰ valore numerico che sarà oggetto di verifica dagli altri partecipanti. In particolare, laddove un *miner* riesca a risolvere il problema matematico ed estrapolare il numero, per ottenere la ricompensa, deve subire il processo di verifica sulla correttezza della soluzione proposta. Correttezza che viene determinata a maggioranza del cinquanta per cento più uno dei nodi, raggiunta la quale il nuovo blocco è aggiunto alla catena.

Premesso che, allo stato attuale, non si comprende neanche chi sia il soggetto al quale sarebbe demandata l'ideazione del problema matematico da risolvere, né con quali criteri, (come può, infatti, un algoritmo essere "neutrale", se è frutto di programmazione?) appare a dir poco paradossale la scelta operativa di rimettere la "certificazione" su base consensuale, di una comunità anonima e ristretta. Al di là delle ombre generate dalla circostanza di una prova troppo complessa da risolvere, la quale taglierebbe fuori potenziali operatori di "buona fede" ma sprovvisti della necessaria capacità computazionale, appare doveroso rilevare che la struttura così congeniata non è certo immune da attacchi e falle di fiducia, laddove un singolo *miner*, così come una minoranza di blocco organizzata, raggiungesse l'ipotetica maggioranza della potenza computazionale richiesta dalla rete per operare, la c.d. *hashrate*. In questo modo, sarebbe infatti possibile ottenere il controllo dell'infrastruttura decisionale, sia in termini di generazione di nuovi anelli sia di influenzare la validazione delle transazioni successive.

Ma anche a voler prescindere da tali problematiche, la questione giuridica davvero irrisolta – e allo stato attuale, irrisolvibile – della *blockchain*, attiene in realtà, alla mancanza di oggettiva certezza sulla genuinità dei dati.

L'accertamento fattuale di un qualsiasi accadimento giuridicamente rilevante, infatti, può essere immesso nel circuito della *blockchain* senza alcun filtro o protezione, generando una situazione di oggettiva incertezza sulla veridicità di quanto assunto.

In questo senso, appare paradigmatico il caso – non più tanto di scuola – delle "nocciole turche" applicato alla filiera agro-alimentare italiana. Poniamo il caso di un'azienda che intenda pubblicizzare una crema spalmabile composta al cento per cento di materie prime italiane e che decida di certificare attraverso la *blockchain* l'italianità integrale delle nocciole impiegate nel processo produttivo.

⁶⁹ L'algoritmo del *Proof of Work*, come è altrettanto noto, rappresenta una delle principali soluzioni per il raggiungimento del consenso ma non è certo l'unica. Ad essa si sommano gli analoghi meccanismi del *Proof of Stake*, del *Delegated Proof of Stake*, del *Proof of Activity* e del *Proof of Authority*, sui quali si rinvia a F. Sarzana, S. Ippolito, M. Nicotra, *Diritto della blockchain, intelligenza artificiale ed IoT*, Milano, 2018.

⁷⁰ Cioè attraverso l'esperimento da parte dei *miner* di tentativi casuali di risoluzione – c.d. *random guessing* – per individuare la soluzione del problema nel rispetto del vincolo di difficoltà così come impostato dal sistema. Cfr. sul punto H. Poston, K. Bennett, *Certified Blockchain Security Professional (CBSP)*, su *Blockchain Training Alliance*, reperibile su blockchaintrainingalliance.com.

Chi e cosa certifica che, effettivamente, le nocciole sono effettivamente piemontesi e non turche?

Al netto di ogni ulteriore considerazione mercatistica e gius-commerciale sull'eventuale scorrettezza di una simile pratica commerciale ingannevole, appare chiaro che il ricorso alla tecnologia basata sui registri distribuiti, anche laddove superasse le evidenziate criticità operativo-informatiche, si limiterà unicamente a bollinare come "integra" l'eventuale nota di carico. Ma chi è che, nella *blockchain*, può fattualmente accertare l'italianità delle nocciole?

Il fatto materiale appena descritto – italianità delle nocciole – rimane ignoto, presunto, sostanzialmente incerto, e questa situazione di incertezza spiega i propri effetti giuridici laddove, riprendendo le parole di Falzea, diventa la «manifestazione o meglio ancora la traduzione sociale del dubbio, ossia un conflitto tra apprezzamenti di due soggetti diversi»⁷¹.

Per stabilire un'eventuale pratica commerciale scorretta o sanzionare una frode alimentare, infatti, come si risolve, nell'esempio proposto, l'eventuale conflitto dell'asimmetria informativa che ne è alla base?

Simili conflitti – prosegue Falzea – rendono impossibile la realizzazione del valore giuridico «fino a quando non intervenga un fatto capace di superare il conflitto e di stabilire, nella contrastante versione della realtà giuridica, la situazione giuridica vera»⁷². L'eliminazione dello stato di incertezza, pertanto, necessita dell'intervento di un mezzo oggettivo in grado di sostituirsi alla situazione di incertezza e ingenerare un legittimo affidamento, spendibile fino a prova contraria.

L'affidabilità e la veridicità di ciò che si certifica, come è stato già osservato in dottrina⁷³, diventano così gli interessi centrali delle dinamiche relazionali, che come tali possono essere assunti dall'ordinamento giuridico e fatti oggetto di regolamentazione e tutela.

Se è sicuramente vero che il monopolio statale sulle certificazioni è ormai eroso, tuttavia, la stessa attività certificativa non è stata, per ciò solo, svuotata di contenuto e non ha certo assunto una diversa connotazione di assoluta neutralità. La differente prospettiva, infatti, si sposta sull'autorevolezza derivante «dalla capacità del certificatore di verificare in modo affidabile i dati dichiarati, in rapporto alla specifica finalità della certificazione»⁷⁴, rispetto alla statica autorità e qualificazione pubblicistica di chi certifica.

Nel caso della *blockchain*, nondimeno, questa prospettiva non sembra essere allo stato attuale giuridicamente possibile, né percorribile, per le ragioni già evidenziate, e, nel permanere di una zona di oggettiva incertezza socialmente apprezz-

⁷¹ A. Falzea, *op. cit.*

⁷² A. Falzea, *op. cit.*

⁷³ A. Benedetti, *Certificazioni "private" e pubblica fiducia*, cit.

⁷⁴ *Ibidem.*

zabile, appare ancora indispensabile il ricorso ad uno strumento formale di accertamento nella valutazione dei fatti di rilevanza giuridica.

Il “mercato” infatti, non è un luogo naturale e auto-produttore della certezza giuridica, ma essendo un *locus artificialis*⁷⁵, la cui artificialità deriva sì da una tecnica del diritto, ma che, in dipendenza delle decisioni politiche è in grado di conferire forma all’economia, occorre pertanto ristabilire il disequilibrio prodotto dalle asimmetrie informative, e quanto queste non possono essere “neutralizzate” dalle stesse logiche volontaristiche di mercato – come è il caso delle molteplici certificazioni volontarie – è necessario l’intervento di un soggetto istituzionalmente fidefaciente⁷⁶, che svolga una funzione di filtro e di garanzia.

Solo attraverso l’accertamento, pertanto, sarà possibile riequilibrare le posizioni mediante la costituzione di un “titolo formale” in grado di sostituirsi alla contestazione, vincolandone il contenuto fattuale ad un elemento certo. In questo senso, riprendendo la nota definizione di Falzea, l’accertamento denota «ogni processo spirituale attivamente orientato verso la situazione spirituale della certezza»⁷⁷ il quale, muovendo da una situazione iniziale di obiettiva incertezza, porta, attraverso l’attività spirituale di chiarificazione della realtà, ad una dichiarazione di scienza munita di efficacia preclusiva.

Rielaborando la nozione di Giannini sui “Fatti di certazione”⁷⁸ appare evidente come questi rientrino nell’ambito della funzione certatrice, cioè dove i pubblici poteri, ossia taluni organi dello Stato, di enti minori, e taluni privati investiti dell’esercizio di tali funzioni, svolgono un’attività che può dirsi primigenia, nel senso che prima di essa non esiste nessuna situazione giuridica⁷⁹. Ma nel contesto dell’analisi giuridica sulla *blockchain*, perderebbe di senso la prospettiva che vorrebbe stigmatizzare la differenza tra fatti di certazione e fatti di accertamento o accla-

⁷⁵ N. Irti, *L’ordine giuridico del mercato*, Bari, 2009

⁷⁶ Cfr. C. Licini, *Il notaio dell’era digitale: riflessioni gius-economiche*, in *Notariato*, 2018, 2, 142 s.

⁷⁷ A. Falzea, *Accertamento*, cit., il quale rileva come poiché il termine accertamento suggerisce immediatamente l’idea di un processo spirituale, nell’accertamento come in ogni processo della realtà noi possiamo opportunamente distinguere tre momenti o stadi: l’inizio, lo svolgimento, il termine. Dallo stadio iniziale, costituito dalla situazione di incertezza, si tratta di pervenire, attraverso lo stadio mediano rappresentato dall’attività di accertamento, allo stadio finale della situazione di certezza.

⁷⁸ M.S. Giannini, *Accertamento (dir. cost. e amm.)*, in *Enc. dir.*, vol. I, Milano, 1958, per il quale i fatti di certazione, nei quali quindi ha rilievo più che il processo intellettuale dell’accertamento, nel senso pregiudicato di acclaramento di fatti – nelle varie più precise forme che esso possa assumere –, il fine di determinare una realtà giuridica per l’innanzi non esistente. I fatti di certazione pervengono ad un’attività giuridica che pur essendo, come per i fatti di accertamento, orientata verso la certezza, non è volta a rimuovere un’incertezza, come situazione reale che rende dubbia la concreta regolazione di comportamenti dei soggetti, ma è volta a qualcosa che è ancor anteriore sotto ogni aspetto – cronistico, logico, intellettuale, materiale, ecc. –, ossia a porre delle statuizioni assertorie giuridicamente valide, tali da comportare un’adesione priva di riserve o quantomeno con possibilità predelimitate di riserve ad un giudizio di realtà, e quindi dar luogo a certezza.

⁷⁹ I fatti di certazione hanno, dunque, tutti, un effetto qualificatorio, che consiste nella creazione di modi di essere della realtà giuridica entro la quale i soggetti agiscono: con locuzione breve, di situazioni giuridiche oggettive.

ramento⁸⁰, laddove, sostanzialmente, il profilo centrale dell'imbarazzo giuridico è dato proprio dalla mancanza di chiarezza iniziale sull'intero contesto di informazioni e dati che vengono processati, al netto di ogni possibile contestazione.

In questo senso, l'analisi sulla produzione di certezze legali, il risultato delle quali, per dirla alla Pugliatti «consiste in un effetto giuridico, ossia nella nascita, modificazione, estinzione di una situazione giuridica»⁸¹, riequilibra il giusto *focus* della prospettiva sugli elementi soggettivi, prima di quelli oggettivi, che l'ordinamento tuttora richiede affinché ci sia il menzionato effetto preclusivo di contestazione e di rimozione dello stato di incertezza. Le organizzazioni sociali e le collettività organizzate, infatti, hanno storicamente demandato a degli intermediari la funzione, altamente fiduciaria, della produzione di certezza giuridica nelle transazioni, con tutte le forme di pubblicità necessarie a questo scopo, attraverso la promozione di una conoscibilità "oggettiva" dei fenomeni giuridicamente rilevanti, che sono resi conoscibili proprio per il tramite di meccanismi trasparenti di opponibilità di atti e supporti documentali, della più varia natura, che rendono possibile proprio la "pubblicità" degli stessi. Ma, in conformità con il combinato disposto degli artt. 2699 e 2700 Cod. Civ., affinché esista un atto pubblico occorre che una norma di legge attribuisca ad un soggetto qualificato come "pubblico ufficiale" il compito di attestare la provenienza dell'atto o i fatti "avvenuti in sua presenza", con l'autorizzazione di attribuirgli pubblica fede.

⁸⁰ La differenza tra i fatti di certazione e i fatti di accertamento è facilmente rilevabile: gli uni e gli altri contengono un accertamento, nel senso pregiuridico di acclaramento di vicende nella loro storicità o nella loro teoresi, ma nei primi l'acclaramento è volto a immettere nel mondo del diritto una realtà per l'innanzi non presente, nei secondi è volto a regolare una realtà già immessa nel mondo del diritto ma effettivamente incerta; i primi operano quindi solo su situazioni oggettive, i secondi su situazioni soggettive; i primi hanno un effetto qualificatorio puro, ossia un effetto giuridicamente del tutto elementare (primigenio), i secondi un effetto preclusivo, ossia un effetto di contenuto complesso che postula l'esistenza di un mondo giuridico già progredito e raffinato; i primi tuttavia hanno, proprio perché ad effetto primigenio, una funzione di base, perché creano modalità, qualità, attributi, di cose e di persone, e quindi identificano generi, specie e individui, onde riuniscono in sé i predicati, apparentemente contrastanti, dell'elementarità più modesta e della necessità più indeclinabile – e perciò se li riserva il potere sovrano in ciascun ordinamento giuridico –; i secondi sono strumenti a disposizione degli operatori giuridici, che essi usano per atto di loro volontà. I fatti (atti) di certazione possono *mediatamente* dar luogo, tramite la situazione oggettiva – o comunque altrimenti si voglia denominare la realtà sottostante a questa locuzione – a fatti che potranno avere effetti costitutivi, dichiarativi, o preclusivi, a seconda del modo com'essi incidono nelle situazioni soggettive. In sé, l'atto (il fatto) di certazione non è né dichiarativo né costitutivo, perché non attiene alle situazioni soggettive.

⁸¹ S. Pugliatti, *Conoscenza e diritto*, Milano, 1961, 30.

7. *Verso una rilettura analogica delle funzioni di hash: le certezze pubbliche del “notaro dell’avvenire”*

La produzione ordinamentale di pubbliche certezze, come è noto, è intesa come una delle funzioni basilari di garanzia dell’intrinseca genuinità dei dati riportati, e tale finalità pubblicistica, pertanto, impone che il supporto materiale che le attesti, provenga da una fonte istituzionalmente obiettiva e imparziale.

In questo senso, per iniziare a rispondere ai quesiti giuridici sollevati dalla *blockchain*, occorre ripensare all’ibrida figura dei notai, sotto l’immutato profilo pubblicistico della funzione essenziale indicata nell’art. 1 della legge notarile (l. 16 febbraio 1913, n. 89), laddove è riconosciuta loro la natura di «pubblici ufficiali istituiti per ricevere gli atti tra vivi e di ultima volontà, attribuire loro pubblica fede, conservarne il deposito, rilasciarne le copie, i certificati e gli estratti». L’esercizio non vuole certo essere una sterile speculazione dogmatica, se solo si considera che, attraverso la *blockchain*, sembrerebbe quasi avverarsi la profezia di Carnelutti sul «notaro automatico dell’avvenire», nel quale – ricorrendo alle macchine elettroniche – «si introdurrà la richiesta e la moneta e dal quale verrà fuori, bell’e pronto il documento contrattuale o testamentario»⁸².

Sebbene una lettura in chiave pubblicistica della funzione notarile non sia certo nuova in dottrina⁸³, appare però indispensabile, in questa sede, rielaborare la cornice giuridica di riferimento dell’attività notarile, per tranquillizzare *ex post* il Maestro e ricollocare nel giusto contesto le tecnologie basate sui registri distribuiti.

La vera forza dell’ufficio notarile, infatti, tale da differenziarlo da qualsiasi *blockchain* attualmente in essere, è data proprio dalla rilevanza all’attività certativa del notaio, laddove questi, per usare le parole di Nigro, comincia «con l’accertare il fatto e rappresentarlo in tutta la sua consistenza e significato»⁸⁴ e passa poi a «situare il fatto nel diritto». Il notaio, quindi, in funzione para e anti-processuale, accerta il fatto e lo fissa in una rappresentazione, attraverso la quale soltanto «vive e vale» nell’ordinamento giuridico vincolando anche il giudice al suo convincimento⁸⁵. Nello specifico, e a dispetto di quanto attualmente è riconosciuto e riconoscibile alla *blockchain*, l’ufficio del notaio, dovendo conformare «fatto e diritto», altro non fa che garantire le parti nel merito, sia fra di loro sia *erga omnes*, tanto sulle dichiarazioni da esse provenienti, quanto sui fatti avvenuti alla presenza di lui.

⁸² F. Carnelutti, *La figura giuridica del notaio*, in *Riv. trim. dir. proc. civ.*, 1950, 925.

⁸³ Si veda, fra le elaborazioni più autorevoli, quella di M. Nigro, *Il notaio nel diritto pubblico*, cit., ovvero quella di F. Carnelutti, *La figura giuridica del notaio*, cit., nonché S. Romano, *La distinzione fra diritto pubblico e privato (e i suoi riflessi nella configurazione dell’ufficio notarile)*, in *Riv. not.*, 1963, 43 s.

⁸⁴ M. Nigro, op. cit., 434.

⁸⁵ M. Nigro, op. cit., 436.

Questa attività del notaio, sostanzialmente documentale – nel senso più proprio del termine – richiama il concetto semi-ancestrale di “cosa autentica”, già definita da Romagnosi come «qualunque atto racchiudente i requisiti voluti dalla legge per far fede delle cose in esso contenute fino ad iscrizione di falso»⁸⁶. Ed è questa la menzionata portata preclusiva sull’incertezza che – per lo meno allo stato attuale – manca alle tecnologie basate sui registri distribuiti. Come già rilevato da Falzea, infatti, la messa fuori contestazione, la sostituzione della situazione giuridica incerta con la situazione giuridica accertata, «null’altro possono significare nella loro versione scientificamente corretta se non precisamente la preclusione di qualsiasi indagine sulla situazione giuridica antecedente al fatto di accertamento e pertanto la irrilevanza di ogni contestazione relativa al contenuto della situazione giuridica accertata sulla base della sua validità storico-giuridica»⁸⁷.

Per di più, a dispetto della *blockchain* – che è imperniata, come visto, su di un sistema sostanzialmente volontaristico e di convenienza – i notai, proprio perché pubblici ufficiali, hanno l’obbligo di esercizio del loro ufficio in modo imparziale, trasparente e posto a garanzia dell’intero ordinamento giuridico, prima delle parti. Rispetto ai *miners*, oltretutto, i notai non rivestono la qualifica di “utenti” della rete di registri di cui fanno parte, ma, anzi, ne custodiscono l’integrità in modo del tutto terzo e disinteressato.

Inoltre, passando all’esegesi di alcune delle più significative disposizioni della legge notarile del 1913, si evincono alcune caratteristiche empiriche perfettamente sovrapponibili ai “nuovi” elementi formali che vorrebbero rappresentare i punti di forza delle tecnologie basate sui registri distribuiti.

L’art. 18, in primo luogo, impone al notaio, prima di assumere l’esercizio delle sue funzioni, di ricevere il sigillo o segno di tabellionato (fornito dal Consiglio notarile) e di scrivere in un registro apposito, tenuto nella segreteria del Consiglio, la propria firma accompagnata dall’impronta dell’anzidetto sigillo.

L’art. 52, in secondo luogo, prescrive che la firma che il notaio appone in fine dell’atto, dev’essere munita dell’impronta del suo sigillo, segno esteriore del *munus* di pubblica fede, talmente importante che l’art. 40 ne disciplina le “sorti” in caso di dismissione⁸⁸.

L’art. 61, in terzo luogo, prescrive che il notaio debba custodire “con esattezza ed in luogo sicuro” sia gli atti da lui ricevuti (compresi gli inventari di tutela

⁸⁶ G.D. Romagnosi, *Principi fondamentali di diritto amministrativo onde tesserne le istituzioni*, Piatì, 1832, 34.

⁸⁷ A. Falzea, op. cit., il quale prosegue rilevando che «dopo il fatto di accertamento una ulteriore contestazione non tanto è vietata quanto è resa irrilevante e perciò è privata della sua forza paralizzatrice della realizzazione del valore giuridico».

⁸⁸ Il sigillo del notaio cessato definitivamente dall’esercizio o trasferito ad altra sede è depositato nell’archivio notarile distrettuale. Il sigillo è reso inutilizzabile, in modo da restare comunque riconoscibile, mediante l’apposizione di un segno sull’incisione a cura del capo dell’archivio.

ed i verbali delle operazioni di divisione giudiziaria) sia gli atti presso di lui depositati per disposizione di legge o a richiesta delle parti.

A questo effetto, l'art. 61 prosegue, prefigurando un sostanziale *hash ante litteram*, che il notaio li rilegherà in volumi (*blocks?*) per ordine cronologico (*time stamping?*) ponendo sul margine di ciascun atto un numero progressivo (*hash*).

L'art. 62 prescrive, in quarto luogo, che il notaio tenga, oltre i registri prescritti da altre leggi, due repertori a colonna – uno per gli atti tra vivi, uno per le ultime volontà – e in essi deve prender nota entro il giorno successivo, senza spazi in bianco ed interlinee, e per ordine di numero di tutti gli atti ricevuti, compresi tra i primi quelli rilasciati in originale, le autenticazioni apposte agli atti privati, e i protesti cambiari. Quanto al menzionato *hash ante litteram*, il repertorio degli atti tra vivi, per ciascuna colonna, deve contenere, tra gli altri⁸⁹, anche il numero progressivo⁹⁰, la data dell'atto e dell'autenticazione – *time stamping* – oltre all'indicazione del Comune in cui l'atto fu ricevuto, in funzione “geo-locatrizzatrice” del diritto applicabile.

Inoltre, in un'ottica di “protezione dati personali” nell'alveo del GDPR – diremmo oggi, in luogo dei più corretti termini di riservatezza deontologica e segretezza professionale – il notaio «non è tenuto a dar visione del repertorio, né copia, certificato od estratto, se non a chi è autorizzato a chiederli dalla legge, dall'autorità giudiziaria avanti la quale verta un giudizio, o, negli altri casi, dal presidente del tribunale, da cui il notaio dipende».

Quanto poi alla distribuzione del registro, occorre rilevare come l'attività notarile preveda già un “registro distribuito” che tenga traccia sia dell'atto rogato o ricevuto dal notaio, sia della copia trasmessa in conservatoria dei registri immobiliari – che dipende dall'Agenzia delle Entrate – e sia della copia nell'archivio distrettuale notarile⁹¹, retto da un conservatore⁹² vigilato dal Ministero di grazia

⁸⁹ La natura dell'atto ricevuto o autenticato; i nomi e cognomi delle parti ed il loro domicilio o la residenza; l'indicazione sommaria delle cose costituenti l'obbietto dell'atto, ed il relativo prezzo e valore, ed ove trattasi di atti che abbiano per oggetto la proprietà od altri diritti reali od il godimento di beni immobili, anche la situazione dei medesimi.

⁹⁰ La serie progressiva dei numeri degli atti e dei repertori, viene continuata fino al giorno in cui il notaio avrà cessato dall'esercizio delle sue funzioni nel distretto in cui è iscritto: e, cambiando residenza in un altro distretto, il notaio dovrà cominciare una nuova numerazione.

⁹¹ Ai sensi dell'art. 65 della legge notarile, il notaio ha l'obbligo di trasmettere all'archivio notarile distrettuale, istituito in ogni Comune sede di tribunale civile, ogni mese, una copia dei repertori limitatamente alle annotazioni degli atti ricevuti nel mese precedente. Tale copia sarà scritta in carta libera, sottoscritta dal notaio, e munita dell'impronta del suo sigillo. Gli atti originari ed i repertori debbono essere custoditi nell'archivio, in luogo separato da quello in cui sono custodite le copie. Le copie devono rilegarsi in volumi corrispondenti ai volumi degli originali di ciascun notaio.

⁹² Il quale, oltre a dover godere della cittadinanza italiana e di “moralità e di condotta incensurate”, è responsabile della custodia e conservazione di tutti i documenti, repertori e sigilli depositati nell'archivio. Esso veglia al regolare andamento del medesimo, all'esatto adempimento degli obblighi imposti ai notari verso l'archivio, e denuncia alla competente autorità le contravvenzioni in cui i notari o altre persone fossero incorse per

e giustizia, e l'amministrazione del quale è addirittura soggetta al controllo della Corte dei conti e del Parlamento.

La rilettura delle funzioni di *hash* in chiave analogica, pone perciò l'attenzione su di un altro aspetto fondamentale dell'analisi giuridica quivi proposta. Si tratta della neutralità tecnologica che il nostro ordinamento, improntato alla libertà delle forme, riconosce alla formazione e conservazione degli atti, e che già a partire dalle leggi Bassanini, con l'art. 15, comma 2, della l. 15 marzo 1997, n. 59, aveva previsto che «Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge», principio poi trasfuso e approfondito nell'attuale Codice dell'Amministrazione digitale.

Ma anche solo in termini di teoria generale, occorre rilevare che la forma "scritta" *ab substantiam* richiesta, ad esempio, dall'art. 1350 Cod. Civ., non significa più forma "cartacea", ben potendo il supporto documentale assumere la connotazione di *file* digitale, e la stessa forma dell'atto pubblico digitale, ormai, è normativamente equiparata al cartaceo⁹³. Anche i registri, già definiti da Giannini come «strumenti costituiti da materiali idonei a ricevere dei fatti grafici»⁹⁴ ben possono assumere la forma digitale, anzi, a mente dell'art. 66-*bis* della legge notarile, tutti i repertori e i registri dei quali è obbligatoria la tenuta per il notaio «sono formati e conservati su supporto informatico», nel rispetto dei principi di cui al Codice dell'Amministrazione digitale, e, avvalendosi dell'infrastruttura informatica all'uopo predisposta e gestita dal Consiglio nazionale del notariato, laddove la relativa registrazione, comporta l'effetto pratico di consentire, che tali atti, costituiscono ad ogni effetto di legge degli originali informatici (*double spending?*) dai quali possono essere tratti duplicati e copie.

inosservanza delle disposizioni concernenti gli archivi. Inoltre, il conservatore rientra nel regime di incompatibilità normativamente previsto a garanzia della funzione archivistica. Infatti, gli impieghi d'archivio sono incompatibili con l'esercizio del notariato e con qualunque altra professione, salvo l'insegnamento di materie giuridiche ed archivistiche. Sono pure incompatibili con qualunque altro pubblico impiego. In più, tanto il conservatore, quanto gli archivisti, sottoarchivisti ed assistenti, debbono fissare la loro residenza nel Comune dove è l'archivio. Il conservatore deve inoltre fare cauzione entro due mesi dalla registrazione del decreto di nomina. La cauzione deve corrispondere a due annualità intere di stipendio e deve essere data o in titoli di rendita del debito pubblico, o in titoli emessi o garantiti dallo Stato, o con deposito di danaro, presso la Cassa dei depositi e prestiti.

⁹³ In tal senso, si veda anche l'art. 47-*bis* della legge notarile, il quale riconosce all'atto pubblico di cui all'art. 2700 Cod. Civ., redatto con procedure informatiche, l'applicabilità delle disposizioni della stessa legge notarile. Così come, l'autenticazione di cui all'articolo 2703, comma 2, Cod. Civ. è regolata, in caso di utilizzo di modalità informatiche, dall'art. 25 del CAD. Quest'ultimo, a seguito della modifica intervenuta con il d.lgs. 13 dicembre 2017, n. 217, ha poi introdotto una nuova modalità di creazione di documenti informatici con la stessa efficacia probatoria di cui all'art. 2702 Cod. Civ., pari a quelli sottoscritti con firma digitale, qualificata o avanzata, qualora rispetti le linee guida dell'AgID, mentre, nei restanti casi, il valore probatorio del documento informatico è rimesso al libero apprezzamento del giudice.

⁹⁴ M.S. Giannini, *Diritto amministrativo*, cit., 994.

Non da ultimo, a chiusura dell'analisi sulla sostanziale insostituibilità della funzione notarile attraverso un'indisciplinata astrazione algoritmica, occorre rilevare come, in caso di errore, nel sistema notarile tradizionale è sempre ammessa la rettifica del contenuto, così come sussiste la protezione sull'integrità del "contenitore" documentale data dall'istituto della querela di falso⁹⁵, *in primis* materiale, che però può estendersi anche sui profili ideologici della relativa rappresentazione. Protezione che, allo stato attuale, risulta del tutto priva la struttura delle tecnologie basate sui registri distribuiti, le quali, semmai, possono aggiungere il loro *quid* crittografico a coronamento dell'integrità esteriore dell'accertamento documentale "analogico", formalizzato su supporto informatico, e non è certo un caso, se, nel 2018, il Consiglio Nazionale del Notariato abbia lanciato lo studio pilota sulla c.d. *Notarchain*⁹⁶, abortito per una sostanziale lacunosità della normativa tecnica di contorno.

8. *Lo stato dell'arte negli altri Paesi: l'incompiuta regolazione del fenomeno*

Il tentativo di risolvere le criticità giuridiche derivanti dall'impiego delle tecnologie basate sui registri distribuiti, non può prescindere dall'analisi delle soluzioni istituzionale adottate da altri ordinamenti giuridici, anche se, allo stato attuale, poco o nulla è stato aggiunto al relativo dibattito sull'inquadramento giuridico-sistematico del fenomeno. Concentrando lo spettro d'indagine agli ordinamenti più affini dell'Europa continentale, e dei sistemi di *common law*, a livello cronologico, la prima presa di posizione nazionale è stata della Francia, che già nel 2016, nell'alveo della c.d. "*loi Sapin 2*" sulla trasparenza, la lotta alla corruzione e la modernizzazione della vita economica, ha provveduto a novellare il *Code monétaire et financier* con la prima *ordonnance* specifica in materia (la n. 2016-520 du 28 avril 2016) relativa ai *bons de caisse*, con la quale ha consentito l'emissione e la registrazione dei *minibons*⁹⁷ su di un «*dispositif d'enregistrement électronique partagé permettant l'authentification*».

⁹⁵ Quale procedimento giurisdizionale, disciplinato dall'art. 221 c.p.c., finalizzato a contestare la veridicità di un atto pubblico oppure di una scrittura privata riconosciuta.

⁹⁶ Già a partire dal 2017, per rispondere alle esigenze di digitalizzazione del Paese e per garantire la sicurezza nelle transazioni, il Notariato ha proposto due applicazioni concrete delle più moderne modalità di archiviazione dei dati digitali: i registri diffusi (*blockchain*) e i registri volontari digitali. In tale contesto, era stato lanciato anche un progetto in *partnership* con IBM per realizzare la *Notarchain*, cioè una piattaforma *blockchain* nella quale le informazioni non fossero gestite da soggetti anonimi, ma dai notai italiani, e con il vantaggio tecnologico di mantenere intatte le potenzialità connesse alla velocità, all'assenza di costi per il cittadino fruitore, alla diffusione su scale mondiale, ovviando alle criticità potenziali di un modello di registro decentrato e privo di controlli sulla veridicità dei dati inseriti. Sul punto, si rinvia alle pubblicazioni del Consiglio Nazionale del Notariato, liberamente consultabili su https://www.notariato.it/sites/default/files/cs_notarchain_13102017.pdf.

⁹⁷ I *minibons* sono dei buoni progettati appositamente per le operazioni di *crowdfunding*.

La modifica del *code monétaire* ha così tentato, senza troppi esiti, di aprire la strada all'inquadramento giuridico della *blockchain*, seppur limitato all'ambito della tracciabilità finanziaria, implementata con la seconda *ordonnance* della materia (la n. 2017-1674 du 8 décembre 2017⁹⁸) relativa all'utilizzo di un «*dispositif d'enregistrement électronique partagé*» per la rappresentazione e la trasmissione dei titoli finanziari, che ha rappresentato il prodromo normativo per la registrazione informatica di titoli, produttiva degli stessi effetti giuridici del deposito in un conto titoli "analogico", successivamente corroborato dalle previsioni del *Décret n° 2018-1226 du 24 décembre 2018*⁹⁹ relativo all'utilizzo del «*dispositif d'enregistrement électronique partagé*» per la rappresentazione e la trasmissione dei titoli finanziari e per l'emissione e la cessione dei *minibons*.

Sulla scia dell'esperienza francese, l'ordinamento maltese ha visto, nella seconda metà del 2018, l'introduzione di tre testi legislativi sulla *Blockchain*, il *Malta Digital Innovation Authority Act*, c.d. MDIA Act; l'*Innovative Technological Arrangement and Services Act*, c.d. ITAS Act; e il *Virtual Financial Asset Act*, c.d. VFA Act.

Senza dubbio, il MDIA Act rappresenta il testo maggiormente significativo, laddove, oltre all'istituzione di un'apposita autorità per l'innovazione digitale¹⁰⁰, contiene la definizione maltese di tecnologia basata sui registri distribuiti (*distributed ledger technology*), quale «*a database system in which information is recorded, consensually shared, and synchronised across a network of multiple nodes, or any variations thereof*» così come descritta nel First Schedule dell'ITAS Act, che la intende come un «*software and architectures which are used in designing and delivering DLT which ordinarily, but not necessarily: (a) uses a distributed, decentralized, shared and, or replicated ledger; (b) may be public or private or hybrids thereof; (c) is permissioned or permissionless or hybrids thereof; (d) is immutable; (e) is protected with cryptography; and (f) is auditable*». Ad ogni modo, al netto di ogni considerazione politica sull'iniziale proposito, successivamente smentito, di realizzare una "*Blockchain Island*" attrattiva di operatori e investimenti internazionali, l'esperienza giuridica maltese non offre particolari spunti di riflessione né un contributo di ordine sistematico ulteriore all'indagine giuridica sull'eventuale funzione certificativa della *blockchain*.

Anche l'ordinamento giuridico tedesco, allo stato attuale, risulta essere privo di un inquadramento sistematico del fenomeno delle tecnologie basate sui

⁹⁸ Cfr. *Ordonnance n° 2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers*, <https://www.legifrance.gouv.fr/affich-Texte.do?cid-Texte=JORFTEXT000036171908&categorieLien=id>.

⁹⁹ Cfr. <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037852460&categorieLien=id>.

¹⁰⁰ Alla quale sono state demandate le funzioni di garanzia e di vigilanza sul corretto uso delle tecnologie basate sui registri distribuiti, dovendo armonizzare le pratiche e gli *standard* informatici tra gli operatori interessati ad insediarsi sull'isola.

registri distribuiti. La Repubblica Federale Tedesca, infatti, ha solamente pubblicato nel settembre 2019 una strategia-quadro sulla *blockchain* ad opera del *Bundesministerium für Wirtschaft und Energie*¹⁰¹. Di particolare interesse, sul fronte normativo, è la partecipazione del *Deutsches Institut für Normung*¹⁰² alla redazione dello *standard* normativo internazionale ISO/TC 307 “*Blockchain and Distributed Ledger Technologies*”, chiamato ad affrontare multi-lateralmente i temi spinosi dell’interoperabilità e della sicurezza informatica delle applicazioni che fanno uso della *blockchain*¹⁰³.

Un evidente vuoto regolamentare permane, infine, nell’ordinamento giuridico spagnolo, laddove, nonostante nel 2018 fosse stata depositata in parlamento la *Proposición no de Ley sobre la introducción de tecnología Blockchain en la Administración Pública en España* (poi decaduta nel 2019), il successivo *Real Decreto-ley 14/2019* ha invertito diametralmente l’approccio in chiave decisamente restrittiva e attendista – ai limiti dell’iconoclastia digitale – prescrivendo che, nei rapporti tra cittadini e P.A., in attesa di una compiuta e specifica regolamentazione comune da parte dell’U.E., non sono ammissibili «*en ningún caso y, por lo tanto, no podrán ser autorizados, los sistemas de identificaciones basados en tecnologías de registro distribuido y los sistemas de firma basados en los anteriores*». In questo senso, la previsione normativa si scontra con le obiezioni sollevate dalla dottrina¹⁰⁴ sull’astratta compatibilità della tecnologia *blockchain* con le disposizioni della *Ley 9/2017 de Contratos del Sector Público*, anche per quanto riguarda gli elevati standard di sicurezza richiesti, sia, più in generale, dall’art. 7 della *Ley Modelo de la CNUDMI sobre Documentos Transmisibles Electrónicos* laddove prevede che «*No se negarán efectos jurídicos, validez ni fuerza ejecutoria a un documento transmisible electrónico por la sola razón de que esté en forma electrónica*», così come, gli artt. 267 e 268 della *Ley*

¹⁰¹ Si veda, al riguardo, il rapporto del Ministero federale tedesco degli Affari Economici e dell’Energia, “*Blockchain Strategy of the Federal Government We Set Out the Course for the Token Economy*” del 18 settembre 2019, consultabile su <https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/blockchain-strategy.html>.

¹⁰² Istituto tedesco per la standardizzazione, ente di diritto privato.

¹⁰³ Cfr. Sul punto “*Blockchain Strategy of the Federal Government We Set Out the Course for the Token Economy*”, 18 settembre 2019, 15, https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/blockchain-strategy.pdf?__blob=publicationFile&v=3.

¹⁰⁴ Sul punto, si veda quantorilevato da M.P. Cárceles, *La utilización del blockchain en los procedimientos de concurrencia competitiva*, in *Revista General de Derecho Administrativo*, nell’ambito del “*Derecho Público, derechos y transparencia ante el uso de algoritmos, inteligencia artificial y big data*”, Iustel, gennaio 2019, per il quale la *blockchain* risulterebbe «*Conforme a lo contemplado en la disp. adic. 15ª.3 LCSP, la presentación de ofertas y solicitudes de participación en los procedimientos de contratación pública se llevará a cabo utilizando medios electrónicos. Blockchain es una tecnología compatible con la mayor parte de las exigencias que las disposiciones adicionales 15ª a 17ª LCSP establecen para su uso, tanto por sus elevados estándares de seguridad como por la necesidad de que los archivos electrónicos que integran los expedientes de contratación en su red estén en formatos abiertos, libres y reutilizables (disp. adic. 16ª.j) LCSP*».

1/2000 de *Enjuiciamiento Civil* consentono già di produrre in giudizio documenti elettronici, purché siano firmati con firma elettronica riconosciuta¹⁰⁵.

Anche l'analisi delle due maggiori tradizioni di *common law* non offre spunti significativi per contribuire all'inquadramento giuridico-sistematico delle tecnologie basate sui registri distribuiti. L'esperienza giuridica inglese, infatti, al momento non fornisce alcuna regolamentazione specifica della *blockchain*, imponendo anche in questo contesto giuridico di ricavare *per relationem* il quadro normativo di riferimento a seconda delle implicazioni pratico-operative derivanti dall'utilizzo della tecnologia, così come è dubbia la possibilità di riconoscerne effetti giuridici¹⁰⁶.

Sul versante americano, invece, i profili di maggiore attenzione normativa per tale tecnologia, a livello di regolamentazione federale degli Stati Uniti, hanno riguardato gli aspetti finanziari degli scambi di criptovalute e sulla prevenzione di ipotesi di riciclaggio¹⁰⁷. I singoli stati dell'unione, invece, si stanno muovendo in ordine sparso sulla possibilità di attribuire una validità giuridica autonoma per la *blockchain*, che vada oltre i profili legati alla circolazione di criptovalute¹⁰⁸.

¹⁰⁵ Cfr. sul punto anche M.Á. Bernal Blay, *Blockchain, Administración y contratación pública*, in *Observatorio de Contratación Pública*, 12 luglio 2018, laddove rileva che «una PNL para la utilización de la tecnología para la prestación de blockchain servicios públicos debería [...] habilitarse la utilización general de “huellas electrónicas” como prueba de existencia de documentos u otros datos, tal y como se hace en materia de contratación pública para la presentación de ofertas [...] introducir la tecnología blockchain en los procedimientos administrativos [...] implementar soluciones de identidad digital soberana (‘self-sovereignidentity’) gestionadas con tecnología blockchain».

¹⁰⁶ Secondo il considerando 132 del *Legal Statement on Crypto assets and Smart contracts* pubblicato dal Parlamento Britannico, infatti, «The ledger cannot however be treated as a definitive record of legal rights unless statute has given it binding legal effect (as is the case with the Land Register). There is at present no such statute applicable to cryptoasset ledgers. This means that if a court is required to consider who owns a particular cryptoasset then it will not be bound by the position in the ledgers», https://135z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/20-19/11/6.60-56_JO_Cryptocurrencies_State-ment_FINAL_WEB_111119-1.pdf.

¹⁰⁷ Quasi a ridosso della deflagrazione della pandemia da Covid-19, infatti, era stato presentato il progetto di legge del 9 marzo 2020 “*Crypto-Currency Act of 2020*” recante la suddivisione dei *digital assets* in tre categorie (crypto-securities, crypto-currencies, e crypto-commodities) identificando il Financial Crimes Enforcement Network, la Securities and Exchange Commission e la Commodity Futures Trading Commission come “*Federal CryptoRegulators*”. Il testo del progetto è liberamente consultabile su <https://www.congress.gov/bill/116th-congress/house-bill/6154/text?q=%7B%22search%22%3A%5B-%22crypto-currency+act%22%5D%7D&r=1&s=2>.

¹⁰⁸ Passando in rassegna a volo d'angelo le principali soluzioni normative dei singoli Stati, occorre segnalare l'Arizona che già nel 2017 ha emanato lo *Statute* § 44-7061, con il quale sono state rese legalmente valide le firme, i documenti e i contratti garantiti dalla tecnologia *blockchain* e lo *Statute* § 11-269.22 del 2018, che ha vietato alle contee di proibire la gestione privata di nodi sulla piattaforma *blockchain*. Degna di nota è anche l'esperienza locale della California, la quale, con il disegno di legge n. 838 del 28 settembre 2018, dopo aver definito le caratteristiche essenziali della *blockchain*, ha autorizzato le società per azioni che non emettono titoli in circolazione quotati in borsa a inserire nel proprio atto costitutivo specifiche disposizioni che consentano la registrazione delle operazioni di emissione, trasferimento e conservazione effettuate dai propri azionisti mediante *blockchain*. Anche il Connecticut, con il disegno di Legge n. 443 del 6 giugno 2018 ha istituito un gruppo di lavoro con il compito di formulare raccomandazioni funzionali a sviluppare un piano generale per favorire la crescita dell'industria *blockchain*. Parimenti, lo Stato del New Jersey ha avviato nel marzo 2018 la *Blockchain Initiative Task Force*, con il compito di individuare i vantaggi derivanti dall'uso della tecnologia nelle operazioni di conservazione dei registri e di erogazione di servizi, attraverso l'implementazione e la predisposizione di registri distribuiti crittografati, sulla falsariga di quanto già in atto di sperimentazione nello stato

9. *Considerazioni conclusive*

Volendo tirare le fila del discorso, occorre iniziare attestarsi su una salda posizione realistica: il fondamento logico del concetto giuridico di accertamento trova la sua ragion d'essere nell'implicazione reciproca che intercorre tra il menzionato effetto preclusivo sulla contestazione¹⁰⁹ e la dichiarazione di "verità" incondizionata da questo derivante, che è universalmente fidefaciente nell'ordinamento. Cercando però di fare chiarezza sull'effettivo valore certificativo da riconoscere alle tecnologie basate sui registri distribuiti, è innegabile rilevare come, allo stato attuale, queste non possano conferire alcuna certezza legale ulteriore rispetto alle mere presunzioni di integrità materiale del registro, e della datazione presuntivamente certa. L'accertamento effettuato tramite gli evidenziati algoritmi, infatti, si pone solo come complicazione procedurale di un esteriore "virtualmente irreversibile" delle trascrizioni digitali, non essendo ammissibile il paracadute di seta pura rappresentato dalla querela di falso, né una rettifica materiale, che sia istituzionalmente confortante¹¹⁰.

La *blockchain* non è, pertanto, – o perlomeno non lo sono sue declinazioni attualmente conosciute – una qualificazione di un fatto ignoto giuridicamente rilevante, né alcun effetto giuridico ulteriore può esserle riconosciuto, a partire da quello preclusivo di incertezza, stante il sostanziale vuoto normativo che la circonda, sia a livello nazionale sia e soprattutto a livello comparato. Sicuramente le relative scritture informatiche potranno entrare nel processo, come generale prova atipica, ma non hanno alcuna portata processualmente vincolate sull'apprezzamento di merito in esse contenute.

Anche l'auspicata adozione delle – ormai famigerate – linee guida dell'AgID, se si limitasse a una regolamentazione di *standard* tecnico-tecnologici, può forse sperare di superare le diverse criticità materiali e operative di funzionamento, ma per certo, la regola tecnica non sostituirebbe mai la regola giuridica sulla produzione di certezze legali (come potrebbe, del resto?).

L'approccio tecnologico dell'ordinamento giuridico deve essere sicuramente laico e neutrale, le forme sono sicuramente libere, ma gli effetti giuridici ad esse ricollegabili non lo sono, specie laddove si manifestano in un presidio documentale a garanzia delle transazioni.

di New York con il Disegno di Legge n. 8793. In questa ricostruzione, appare poco significativa, per non dire giuridicamente irrilevante, l'indagine sul Disegno di Legge n. 765 del Vermont laddove prevede, al fine di promuovere l'efficienza degli apparati amministrativi e la produttività dei processi produttivi pubblici e privati l'implementazione di strategie in materia di *Blockchain*.

¹⁰⁹ Rende cioè irrilevante l'alternativa possibile, della conformità o della difformità, del senso positivo o negativo, di quella determinata realtà giuridica alla quale l'effetto fa riferimento, e quindi l'eliminazione di un possibile conflitto di apprezzamenti intorno ad una realtà giuridica passata.

¹¹⁰ Le ipotesi di rettifica di un passaggio della catena di blocchi, infatti, come visto *supra*, par. 6, sono possibili previo consenso maggioritario, e generano comunque un "bivio" dell'infrastruttura.

La scienza economica ha già da tempo acquisito e compreso la rilevanza del problema dei costi sociali di transazione, volti alla rimozione delle asimmetrie informative¹¹¹, configurando la “fiducia” nella qualità delle informazioni circolanti come un bene pubblico in senso economico¹¹². In questo senso, sebbene anche l'accertamento notarile sia sicuramente un “costo di transazione”, tuttavia, varrebbe la pena richiamare l'innegabile considerazione, secondo la quale «il rassicurante paradigma notarile ha un costo minore della spesa che, a posteriori e senza notaio, si spenderebbe per ricostruire la certezza del diritto»¹¹³.

Come già rilevato da chi ha contribuito alla trattazione sistematica del tema della certezza, «le certezze sono pubbliche non perché siano rette da norme di diritto pubblico, ma perché creano un legittimo affidamento nel cittadino che, al di là del valore giuridico, ha valore eminentemente pratico»¹¹⁴.

La dottrina giuridica che sia consapevole della sua funzione e delle sue responsabilità, insegna Calamandrei, non può mai dimenticare i fini pratici a cui è necessariamente preordinata l'opera del giurista: non solo dell'avvocato o del giudice, ma anche del giurista scienziato¹¹⁵. I giuristi, infatti, non possono permettersi il “lusso della fantasia”¹¹⁶ perché gli errori teorici d'oggi creano la realtà di domani. In questo senso, è necessario abbandonare le “mitologie giuridiche”¹¹⁷ enfaticamente una de-regolamentata modernità pan-digitale e contrastare le derive marinettiane tendenti al febbrile futurismo giuridico, slegato da qualsiasi substrato di consapevole maturità concettuale¹¹⁸ e diretto solo ad annichilire l'erroneamente supposto “passatismo statale” nella regolamentazione dei fatti economici.

¹¹¹ Sui costi di transazione, cfr. R.H. Coase, *The problem of social cost*, in *Journal of law and Economics*, 3, 1960, 1 s.; J. Stiglitz, *Economia del settore pubblico*, Milano, 2003, 65, che giustifica l'intervento pubblico nell'economia a correzione delle asimmetrie informative.

¹¹² P. Dasgupta, *La fiducia come bene economico*, in D. Gambetta (a cura di), *Le strategie della fiducia*, Torino, 1989, 63 s., nonché A. Benedetti, op. cit., spec. 29.

¹¹³ Rileva sul punto C. Licini, *Il notaio dell'era digitale: riflessioni gius-economiche*, cit., 144.

¹¹⁴ A. Fioritto, op. cit., spec. 110, e la giurisprudenza ivi riportata in nota 120.

¹¹⁵ P. Calamandrei, *La certezza del diritto e le responsabilità della dottrina*, in *Riv. dir. comm.*, 1942, I, 345, per il quale «La scienza giuridica deve servire a rendere più agevole e più facile l'applicazione della norma al caso pratico, ad aumentare, colle suesistemazioni razionali, il grado di certezza del diritto, cioè a rendere sempre più intelligibile la portata delle regole prestabilite dal legislatore all'agire umano ed a mettere il singolo in condizione di calcolare in anticipo, con previsioni sempre più sicure, le conseguenze giuridiche delle proprie azioni».

¹¹⁶ Calamandrei, op. cit., 349, per il quale «Si può usar sopportazione verso il “letterato puro”, perché, alla fin dei conti, è un seccatore innocuo ma il “giurista puro”, che vuole disquisire di diritto senza ascoltarne le ragioni pratiche, è un malanno che con queste sue fantasticherie rischia proprio di distruggere quel diritto di cui egli si bravamente s'infranca a dissertare: e bisogna pur ricordargli che il diritto non può essere materia di svagata dilettazione intellettuale, perché vi circolano dentro, in ogni giuntura, le lacrime e il sangue degli uomini vivi».

¹¹⁷ Si veda, in tal senso, la voce “mitologia giuridica” di Santi Romano, *Frammenti di un dizionario giuridico*, Milano, 1983, spec. 127, laddove il Maestro rileva come il mito sia «una nonverità, un errore, una “inopia”, ma è anche immaginazione, una immaginazione “favolosa” (mito, infatti, originariamente, non significa che favola), che ha potuto spesso, come è noto, essere riaccostata alla poesia o alla “sapienza poetica”, nonché la rielaborazione di P. Grossi, *Mitologie giuridiche della modernità*, Milano, 2005.

¹¹⁸ Come insegna A. Falzea, *Ricerche di teoria generale del diritto e di dogmatica, Teoria generale del diritto*, Milano, 1999, 17, «il diritto deve prendere posizione, esigendo che si producano e si riconoscano effetti giu-

Pertanto, al pari di quanto sta avvenendo – o per lo meno dovrebbe avvenire – sulla natura giuridica delle criptovalute, quale prodotto e presupposto “materiale” di operatività delle tecnologie basate sui registri distribuiti, il relativo dibattito giuridico impone realmente la riflessione sulla necessaria presenza dei pubblici poteri nella regolazione dei fatti economici. Entrando nel vivo della materia, infatti, appare chiara l’esigenza di fondo di garantire delle “certezze relazionali” per la collettività (informatica e non) che assume un rilievo decisivo nella regolazione delle attività economiche che sono alla base delle transazioni, ma questa operazione, si sa, altro non è che l’attività “ordinativa” dei pubblici poteri così come formulata da Giannini¹¹⁹.

Nella stessa prospettiva di garantire, il più possibile, una certezza giuridico-relazionale delle transazioni, appare azzardato ritenere che la rete informatica non debba avere alcun controllo giuridico di garanzia, alcuna normativa di riferimento o, ancor peggio, di ritenere necessaria la ricerca di un ordinamento speciale retto da una idealizzante *lex informatica*, dal sapore anacronistico¹²⁰ al pari dell’omologa *lex cryptographic* invocata quale regolamentazione privatistica di matrice esclusivamente tecnica, disancorata dalla normazione statale, e del tutto avulsa e autonoma da questa sol perché “condivisa” da tutta la comunità informatica¹²¹.

A una simile impostazione metodologica, tuttavia, basterebbe richiamare la considerazione secondo la quale «a poco giova disporre di algoritmi invincibili se poi il collegamento tra mondo reale e mondo crittografico non può essere gestito con la medesima affidabilità»¹²².

In questo senso, una tentativo di soluzione intermedia per salvare le “capre” della crittografia informatica, con i “cavoli” della certezza ordinamentale, può essere la predisposizione di una *blockchain* “giuridicamente pubblica”, nel senso di statale, vigilata e garantita – in una parola: *permissioned*, cioè privata in senso informatico – e che operi come “pubblica depositaria” della funzione certificatrice nel senso

ridici».

¹¹⁹ M.S. Giannini, *Diritto pubblico dell’economia*, Bologna, 1995, spec. 47.

¹²⁰ Sul punto, si vedano le considerazioni di R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, in *Texas Law Review*, February 1998, Vol. 76, N° 3, 552 s., il quale ritiene, alla base della teoria, fondamentale il condizionamento che la tecnologia eserciterebbe, attraverso regole tecnologiche interne alla rete stessa, non soltanto nelle modalità di trasmissione delle informazioni, ma anche su scelte che condizionano la disciplina del rapporto che è però, sostanzialmente privo della cornice normativa statale e rimesso, sostanzialmente, a un dubbio controllo di tipo informatico.

¹²¹ Cfr. sul punto P. de Filippi, A. Wright, *Blockchain and Law, The Rule of Code*, Cambridge, 2018, nonché F. Faini, *Blockchain e diritto: la “catena di valore” tra documenti informatici, smart contracts e data protection*, in *Resp. civ. e prev.*, 2020, 1, 297 s., per la quale «Il diritto deve essere capace di governare la tecnologia e quindi anche le sue espressioni, quali la *blockchain* e quella che è stata definita *lexcryptographica*, raggiungendo un difficile equilibrio, che sia capace di non limitare lo sviluppo tecnologico, ma parimenti riesca a non determinare la prevalenza della tecnologia sulla regolazione giuridica. Di conseguenza, nel disciplinare la tecnologia, il diritto deve riuscire a non rendere tutto ciò che è possibile grazie all’evoluzione tecnologica, solo per questo, giuridicamente legittimo, garantendo il rispetto dei principi dell’ordinamento e la tutela dei diritti previsti».

¹²² U. Bechini, *Da Berlino a Dublino e Pechino*, cit., spec. 1181

proprio del termine, soggetta alla regolamentazione mista tra tecnologia e diritto. In attesa di un provvedimento legislativo che attribuisca “fede pubblica fino a que-rela di falso” ai fatti giuridicamente rilevanti che vengano trascritti nella *blockchain*, appare per il momento sufficientemente bastevole concentrarsi sulla individuazione normativa delle modalità di scelta dei soggetti coinvolti nel processo di verifica-zione, sulle modalità di scrittura delle regole matematico-informatiche di operati-vità e sulla garanzia di tracciabilità dei flussi di informazioni. Non da ultimo – ma questo è un problema forse “solo” informatico – sarà necessario prevedere dei mec-canismi di risoluzione interna delle controversie sulla ricerca del “consenso”, impo-nendo se del caso anche la trascrizione coatta nel registro distribuito come l’eventuale rettifica delle trascrizioni erronee o infedeli, e per farlo, è necessaria la presen-za di un intermediario centralizzato, che sia investito di un chiaro mandato in tal senso e sottoposto alla vigilanza prudenziale di un’ autorità, fosse anche della stes-sa AgID. Tale soggetto, allo stato attuale dello sviluppo tecnologico, ben può esse-re un operatore di mercato con personalità giuridica, altamente qualificato, sia sul profilo tecnico, sia sul profilo “fiduciario” riposto dall’utenza.

La svolta tecnologica digitale, seppur irreversibilmente in atto – complice anche la sferzata distanziatrice inevitabilmente apportata dall’emergenza epide-miologica da Coronavirus – impone delle innegabili esigenze di tracciamento e di protezione di tutti quegli interessi pubblici che sono alla base della certezza rela-zionale delle transazioni. La progressiva transizione verso il digitale, quindi, non deve consentire di snaturare i principi cardine della scienza giuridica, così come non deve permettere che delle considerazioni meta-giuridiche possano essere tra-sposte tali e quali sul piano giuridico, anche se non corrispondono ai suoi canoni specifici. Il cambiamento è inevitabile, ma, per dirla alla Giannini, «Le cose cam-biano non per volontà degli uomini, ma perché i sistemi si modificano con l’ap-porto di una serie di volontà, alcune delle quali puramente derivate»¹²³. Al giu-rista, e allo studioso, è pertanto demandato il compito di offrire – o per lo meno tentare – delle risposte che riportino ordine concettuale alle eccessive fughe in avanti della tecnologia¹²⁴.

¹²³ M.S. Giannini, *Relazione*, (Atti del Convegno, Perugia, 9-10 ottobre 1971), in *Urbanistica e regio-ni*, 1971, 25.

¹²⁴ La necessaria economia del presente contributo non consente ulteriori approfondimenti e conside-razioni su di un tema così vasto come il delicato rapporto tra diritto e tecnologia. Nella consapevolezza di tale limite, si rinvia *ex multis* V. Knapp, *L’applicabilità della cibernetica al diritto*, Torino, 1978; V. Frosini, *Il dirit-to nella società tecnologica*, Milano, 1981; N. Irti, E. Severino, *Dialogo su diritto e tecnica*, cit., 2001; G. Pascuzzi, *Il diritto dell’era digitale*, Bologna, 2002; G. Finocchiaro, *Riflessioni su diritto e tecnica*, cit., nonché, da ultimo, G. Corasaniti, *Il diritto nella società digitale*, Milano, 2018.

Certezza, consenso e certificazioni informatiche: problemi e prospettive di un approccio giuridico al fenomeno delle tecnologie basate sui registri distribuiti

La *blockchain*, come è noto, rappresenta l'ultimo stadio evolutivo dei sistemi di crittografia informatica, i quali, applicati al complesso dei c.d. registri distribuiti, sembrerebbero poter offrire un servizio di tendenziale "unicità" dei *file* circolanti sulla rete informatica. Questi ultimi, infatti, una volta processati attraverso le funzioni di *hash*, possono essere trascritti nel libro mastro digitale della *blockchain*, il c.d. *ledger*, che è decentralizzato su più nodi, e questa distribuzione simultanea di informazioni, unita ai meccanismi di consenso informatico rimesso all'algoritmo di programmazione, sembrerebbero poter consentire una sostanziale "certezza" sulle informazioni così veicolate tra gli utenti, senza necessità di ricorrere ad alcun intermediario istituzionale che svolga funzioni notarili. Al netto della soluzione così escogitata, tuttavia, gli effetti giuridici riconosciuti dal decreto semplificazioni, allo stato attuale, non sembrerebbero altrettanto confortanti nel riconoscere a tale tecnologia una funzione di tipo certificativo, sia in termini di effettiva "certezza legale" e sia di fidejacentza generalizzata.

Certainty, consensus and IT certifications: problems and perspectives of a legal approach to the distributed ledgers technologies

The blockchain, as is known, represents the last evolutionary stage of computer cryptography systems, which, applied to the complex of so-called distributed ledgers, it would seem to be able to offer a sort of "uniqueness" of the files circulating on the computer network.

In fact, once processed through the hash functions, they can be transcribed into the digital ledger, so-called. ledger, which is decentralized on multiple nodes, and this simultaneous distribution of information, combined with the computer consensus mechanisms given to the programming algorithm, would seem to be able to allow substantial "certainty" on the information conveyed between users, without the need to resort to any institutional intermediary carrying out notary functions. Despite the solution thus conceived, however, the legal effects recognized by the simplification decree, at present, do not seem as comforting in recognizing this technology as a certification function, both in terms of effective "legal certainty" and generalized reliability.