

queste istituzioni

**Criptovalute, blockchain
e problematiche**

Antonio Saporito

Numero 4/2025
31 dicembre 2025

Criptovalute, blockchain e problematiche

di Antonio Saporito*

Sommario

1. Natura giuridica delle criptovalute. – 2. Definizioni e disciplina giuridica. – 3. Disciplina pubblicistica: trattamento fiscale e norme penali. – 3.1 Profili di rilevanza penale delle criptovalute. – 3.2 Disciplina fiscale e reati tributari. – 4. Bitcoin e Blockchain Technology. – 4.1. La Blockchain: la necessità di colmare il vuoto normativo. – 5. La tokenizzazione della ricchezza. – 6. Blockchain e problematiche giuridiche: coordinamento con la normativa in materia di documenti informatici, validazione temporale e protezione dei dati personali.

Sintesi

Il saggio analizza in modo sistematico le criptovalute e la tecnologia blockchain, mettendone in luce le principali problematiche giuridiche. Dopo aver esaminato la controversa natura giuridica delle criptovalute e le definizioni normative offerte dal legislatore nazionale ed europeo, l'autore approfondisce il quadro della disciplina pubblicistica, con particolare attenzione ai profili penalistici e fiscali. Viene evidenziato come le caratteristiche di decentralizzazione e anonimato favoriscano il riciclaggio, l'autoriciclaggio e altri reati informatici, oltre a porre rilevanti questioni di tracciabilità dei flussi finanziari. Ampio spazio è dedicato alla tecnologia blockchain, al suo funzionamento e alle potenzialità di disintermediazione, nonché al persistente vuoto normativo che ne accompagna l'utilizzo. Il contributo affronta inoltre il fenomeno della tokenizzazione della ricchezza, mettendone in luce le criticità rispetto alle categorie civilistiche tradizionali. In conclusione, il saggio sottolinea la necessità di un coordinamento normativo, soprattutto in materia di validazione temporale e protezione dei dati personali, al fine di garantire certezza del diritto e tutela effettiva dei diritti fondamentali.

Abstract

The essay provides a comprehensive analysis of cryptocurrencies and blockchain technology, highlighting their main legal issues. After examining the controversial legal nature of cryptocurrencies and the definitions offered by national and European legislation, the author focuses on public law aspects, with particular attention to criminal and tax profiles. The study shows how decentralization and anonymity facilitate money laundering, self-laundering, and other cybercrimes, while also raising serious concerns regarding the traceability of financial flows. Significant attention is devoted to blockchain technology, its functioning, its potential for disintermediation, and the persistent regulatory gaps surrounding its use. The paper also addresses the phenomenon of wealth tokenization, emphasizing its tensions with traditional civil law categories. The contribution concludes by stressing the need for regulatory coordination, especially in relation to time validation and personal data protection, in order to ensure legal certainty and effective protection of fundamental rights.

Parole chiave

Criptovalute, Blockchain, Riciclaggio e reati informatici, Tokenizzazione della ricchezza, Protezione dei dati personali.

Keywords

Cryptocurrencies, Blockchain, Money laundering and cybercrime, Wealth tokenization, Personal data protection.

* Dottore di ricerca e docente a contratto presso l'Università telematica Pegaso.

1. Natura giuridica delle criptovalute.

Una risalente pronuncia del Tribunale di Verona qualificava i bitcoin come “strumenti finanziari”, ritenendo che, nel caso in esame, le valute virtuali svolgessero essenzialmente la funzione di strumenti di investimento¹.

La qualificazione del giudice veneto ha trovato conferma anche in altre pronunce successive da parte della Corte di Cassazione² che, in una recente sentenza le ha definite “prodotti finanziari”, ravvisando il reato di abusivismo finanziario, di cui all’articolo 166, comma 1, lettera c), del Tuf (decreto legislativo 24 febbraio 1998 n. 58), nel caso di violazione degli adempimenti previsti dall’art. artt. 91 e ss. di cui al Testo unico delle disposizioni in materia di intermediazione finanziaria (Tuf)³.

La giurisprudenza definisce “prodotto finanziario”, «il contratto in cui una società proponga al pubblico il “blocco” di una somma per un anno in prospettiva di un guadagno, mediante un meccanismo negoziale consistente nella consegna in affidamento all’investitore di un diamante del valore ipotetico di mille euro, chiuso in un involucro sigillato, contro il versamento in denaro di un identico importo, con l’impegno della società di “riprendersi” il prezioso dopo dodici mesi e di restituire il capitale maggiorato di ottanta euro, senza alcun’altra prestazione a carico dell’investitore, prevalendo in detta operazione gli elementi del credito fruttifero e della garanzia rispetto a quello della custodia, e sussistendo, altresì, il “rischio emittente” legato all’incertezza sulla capacità della società di restituire il tantumdem con l’incremento promesso»⁴.

In base ad un diverso orientamento, le criptovalute sarebbero dei beni giuridici, ex art. 810 c.c., qualificazione osteggiata da chi, ritenendo la nozione legata all’aspetto della corporeità, non ritiene che nel novero possano farsi rientrare quelle entità o risorse incorporali, come le criptovalute, essendo queste delle “stringhe di dati informatici”. Solo una parte minoritaria della dottrina tende ad interpretare il concetto di “cose”, enucleato nella norma del Codice civile, sia in senso naturalistico che giuridico, estendendolo sino a ricomprendere anche creazioni inventive e idee, tecniche o artistiche⁵. Nello stesso senso sembra essere orientato anche il legislatore europeo⁶, per il quale le criptovalute sono mezzi di scambio e, per poter essere tali, sono prima di tutto beni

¹ Trib. Verona, Sez. II civ., 24 gennaio 2017, in *Banca Borsa Titoli di Credito*, fasc. 4, 2014, pagg. 471-482 con nota di M. PASSARETTA, *Bitcoin: il leading case italiano*.

² P. IEMMA, N. CUPPINI, *La qualificazione giuridica delle criptovalute: affermazioni sicure e caute diffidenze*, in *dirittobancario.it*, 8 marzo 2018.

³ Cassazione penale sez. II, 17 settembre 2020, n.26807, con nota di F. AGNINO, *Vendita di bitcoin e intermediazione finanziaria abusiva*; in *Giurisprudenza Commerciale*, fasc.4, 2022, pag. 929, con nota di F. CONSULICH, *Il diritto penale nell’età del crypto-oro. Gli elementi normativi della fattispecie di abusivismo finanziario tra monete virtuali e investimenti reali*.

⁴ Cassazione civile sez. II, 05 febbraio 2013, n.2736, in *Giust. Civ.*, mass., 2013.

⁵ In tal senso, G. RINALDI, *Approcci normativi e qualificazione giuridica delle criptomonete*, in *Contratto e Impresa*, n. 1 (2019), pag. 291; A. TRABUCCHI, *Istituzioni di diritto civile*, Padova, 2007, pag. 528.

⁶ P. IEMMA, N. CUPPINI, *La qualificazione giuridica delle criptovalute: affermazioni sicure e caute diffidenze*, op. cit.

in senso giuridico⁷ e la Sezione fallimentare del Tribunale di Firenze che, nella sentenza n. 18 del 21 gennaio 2019, ne ha parlato come di «un bene, oggetto di trasferimenti e transazioni»⁸.

Un terzo orientamento ha cercato di ricondurre le criptovalute tra le opere dell'intelletto, pur essendo esse prive del carattere della creatività proprio delle opere artistiche o delle invenzioni industriali. Secondo Burlone e De Caria, «l'acquisto della proprietà a titolo originario di uno o più Bitcoin avviene tramite l'impiego di risorse da un lato economiche, dall'altro lato "intellettuali", certamente non in senso stretto (dal momento che le operazioni vengono compiute da macchine), ma pur sempre estrinsecantisi nella soluzione di un problema e nella creazione di un bene nuovo, prima non esistente, univoco, e avente la caratteristica di essere privo di una materialità intrinseca»⁹, conclusione avversata da quanti ritengono che, l'estrazione di bitcoin non sia affatto un processo creativo intellettuale¹⁰.

Infine, le valute virtuali sono state equiparate alle *commodity*, ai derivati e ai documenti informatici¹¹.

2. Definizioni e disciplina giuridica.

Dal 2008 si è assistito ad una proliferazione delle criptovalute, sia sotto il profilo qualitativo che quantitativo¹². Proprio l'estrema varietà di esse ha indotto il legislatore a codificarne una definizione che, tuttavia, non ha chiarito i dubbi circa l'effettiva natura giuridica di tali prodotti, trattandosi, come vedremo di definizioni ampie¹³.

L'art. 1, 2° comma, lett. qq), d.lgs. 21-11-2007, n. 231, così come modificato dall'art. 1, d.lgs. 25-5-2017, n. 90, definisce la valuta virtuale come «rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente»¹⁴.

⁷ Si veda la Direttiva 2018/843.

⁸ Tribunale Firenze sez. fallimentare, 21 gennaio 2019, n.18, in *Banca Borsa Titoli di Credito*, fasc.3, 2021, pag. 399, con nota di V. DE STASIO, *Prestazione di servizi di portafoglio digitale relativi alla valuta virtuale "Nanocoin" e qualificazione del rapporto tra prestatore e utente*.

⁹ P.L. BURLONE, R. DE CARIA, *Bitcoin e le altre criptomonete. Inquadramento giuridico e fiscale*, Istituto Bruno Leoni, 234, aprile, Torino, 2014.

¹⁰ G. J. SICIGNANO, *Bitcoin e riciclaggio*, Torino, 2019, pag. 90 ss.

¹¹ Per approfondimenti, si rinvia a G. J. SICIGNANO, *Bitcoin e riciclaggio*, op. cit., pag. 69 ss.

¹² C. PERNICE, *Criptovalute, tra legislazione vigente e diritto vivente*, in *Ianus, Diritto e Finanza*, 20, 2020, pag. 44

¹³ C. PERNICE, op. cit., 46; M. NICOTRA, *Criptovalute*, in AA.VV., *Smart Contract, criptovalute e blockchain*, 2021, pag. 124,

¹⁴ M. CIAN, *La criptovaluta - alle radici dell'idea giuridica di denaro attraverso la tecnologia: spunti preliminari*, in *Banca Borsa Titoli di Credito*, fasc.3, 1° giugno 2019, pag. 315; A. VICECONTE, *La disciplina applicabile alle criptovalute*, in *IUS*, 12 maggio 2021.

Similmente, l'art. 1, punto 2, lett. d), dir. UE 2018/843, a modifica dell'art. 3, dir. UE 2015/849, designa, con la locuzione valute virtuali, «una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è necessariamente legata a una valuta legalmente istituita, non possiede lo status giuridico di valuta o moneta, ma è accettata da persone fisiche e giuridiche come mezzo di scambio e può essere trasferita, memorizzata e scambiata elettronicamente».

Le disposizioni riportate mettono in evidenza alcune peculiarità delle criptovalute; anzitutto, il riferimento alla rappresentazione digitale di valore da intendersi in una duplice accezione: che il token emesso su blockchain abbia un valore intrinseco, ovvero sia rappresentativo di un valore monetario o sia strumentale all'esercizio di un diritto; che, altrimenti, il token abbia un valore derivante dal cambio con la moneta corrente.

Le predette definizioni tendono, inoltre, a mettere in evidenza l'impossibilità di ricondurre la criptovaluta al potere dello Stato; dunque, in mancanza di riconoscimento statale, la medesima non possiede lo status giuridico di valuta o moneta¹⁵.

Non essendovi alcun vincolo di cambio tra la valuta virtuale e la moneta corrente, si esclude la coincidenza con le *central bank digital currencies*, ovvero monete aventi corso legale, emesse da banche centrali o commerciali, riprodotte sul piano digitale delle monete fiat¹⁶.

In ultimo, si evidenzia che la valuta virtuale può costituire oggetto di scambio, tramite elaborazione elettronica, nonché costituire mezzo solutorio, purché sia accettata come tale dalle parti in via convenzionale¹⁷.

Per definire meglio il concetto di “criptovalute” è necessario introdurre e soffermarsi anche su quello di moneta elettronica, contenuto nella direttiva 2009/110/CE, in base alla quale si tratta del «valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso dietro ricevimento di fondi per effettuare operazioni di pagamento ai sensi dell'articolo 4, punto 5), della dir. 2007/64/CE e che sia accettato da persone fisiche o giuridiche diverse dall'emittente di moneta elettronica». In base alla Direttiva, sono autorizzati ad emettere moneta elettronica «solo gli istituti bancari e postali, gli istituti di moneta elettronica, le banche centrali nazionali e la Banca centrale europea, gli Stati membri o le rispettive autorità regionali e locali agenti in veste di autorità pubblica»¹⁸.

¹⁵ M. NICOTRA, *Criptovalute*, op. cit., pag. 124

¹⁶ C. PERNICE, *Criptovalute, tra legislazione vigente e diritto vivente*, op. cit., pag. 47

¹⁷ M. NICOTRA, *Criptovalute*, op. cit., pag. 124

¹⁸ C. ZONILE, *La regolamentazione internazionale ed europea di contrasto all'uso di valute virtuali da parte della criminalità transnazionale*, in *Rivista di Diritto Internazionale*, fasc.1, 1° marzo 2019, pag. 137; V. DE STASIO, *Verso un concetto europeo di moneta legale: valute virtuali, monete complementari e regole di adempimento in Banca Borsa Titoli di Credito*, fasc.6, 1° dicembre 2018, pag. 747

Dal momento che la valuta virtuale è priva dello status giuridico di moneta, le criptovalute non possono assimilarsi alla moneta elettronica¹⁹.

Sotto il profilo etimologico può osservarsi che il termine criptovaluta si compone di due elementi: cripto e valuta: il primo indica che si è in presenza di un compendio “crittografato”²⁰, per cui la criptovaluta non appare visibile o utilizzabile se non conoscendo le relative chiavi di accesso, rispettivamente pubblica e privata; il secondo, invece, ne indica la funzione: le criptovalute configurano un sistema di pagamento, che si avvale di una rete di soggetti paritari (*peer to peer*), avulso da qualsivoglia regolamentazione specifica o Autorità centrale di governo²¹.

La decentralizzazione è resa possibile dall’impiego della *Distributed Ledger Technology*; ne è un esempio la tecnologia *blockchain* su cui si basano i *bitcoin*²².

Le criptovalute possono essere conservate, in primo luogo, su un *hardware wallet*, ovvero un dispositivo elettronico che permette l’archiviazione e la conservazione *off-line* delle chiavi private e di firmare le proprie transazioni; secondariamente, su un *software wallet*, ovvero un supporto esterno installabile su device²³; infine, su un *web wallet*, creabile online su portali denominati *wallet providers*, assimilabili ai cc.dd. *account exchange*, ossia conti aperti per l’acquisto e la vendita di criptovalute. I *wallet online* presuppongono una registrazione ad un sito web, fornendo i propri dati personali; la gestione dei propri indirizzi e della valuta virtuale è completamente demandata al *provider* che detiene le chiavi private. È sufficiente, in tal caso, conoscere le credenziali d’accesso al sito per gestire le criptovalute da qualsivoglia dispositivo.

In assenza di specifica regolamentazione in tema di valute virtuali nel nostro ed in altri ordinamenti, sono diversi gli istituti che sono potenzialmente richiamabili per analogia laddove si ponesse un problema operativo nel sistema di scambi di moneta virtuale.

Sia le norme del diritto civile sia quelle del diritto commerciale offrono alcuni importanti strumenti di regolazione dell’uso dei Bitcoin tra privati. Può essere rilevante, ad esempio, la disciplina in tema di trasferimenti bancari, così come la più generale disciplina in tema di trasferimento di fondi, che possono essere estese ai trasferimenti di “monete virtuali” laddove sia necessario, ad esempio, stabilire il momento a partire dal quale un pagamento può considerarsi “eseguito” oppure la disciplina in tema di storno di un pagamento erroneamente trasmesso²⁴.

¹⁹ Banca d’Italia, *Comunicazione* del 30-1-2015, sulle Valute virtuali. Sul punto, G. BEFANI, *Contributo allo studio sulle criptovalute come oggetto di rapporti giuridici*, in *Il diritto dell’economia*, anno 65, n. 100 (3 2019), pag. 392.

²⁰ G. BEFANI, *Contributo allo studio sulle criptovalute come oggetto di rapporti giuridici*, op. cit., pag. 398

²¹ Si vedano, CONSOB, *Le criptovalute: che cosa sono e quali rischi si corrono*, in *consob.it.*; AGENZIA DELLE ENTRATE, *Risoluzione n. 72 del 2 settembre del 2016*.

²² P. DAL CHECCO, F. PASCUCCI, G. RECCIA, M. STELLA, *Bitcoin forensics e intelligence sulla blockchain: Aspetti giuridici, economici, fiscali ed investigativi delle criptovalute*, Roma, 2019, pag. 15-16.

²³ I *software wallet*, per converso, consentono la gestione in locale delle criptovalute, nonché la disponibilità delle chiavi private da parte dell’utente.

²⁴ Cfr. R. BOLLEN, “*The Legal Status of Online Currencies: Are Bitcoins the Future?*”, in *Journal of Banking and Finance Law and Practice*, 2013, pag. 20; G. ARANGÜENA, “*Bitcoin: una sfida per policymakers e regolatori*”, in *Diritto mercato tecnologia*, Quaderno Anno IV, n.1, 2014, pag. 23

Non è invece applicabile la disciplina sui sistemi di pagamento prevista ad esempio dalla Direttiva 64/2007/CE (cd. Direttiva PSD) in quanto essendo la moneta elettronica esclusa dalla sua sfera di applicazione, se ne deduce per analogia, *a fortiori* l'inapplicabilità per le monete virtuali (prive di quelle forme di sorveglianza all'emissione cui è invece sottoposta la prima).

Tra le norme positive invocabili non va invece dimenticata la disciplina in materia contrattuale, soprattutto se e laddove si considerino i Bitcoin alla stregua di “monete complementari”. In questo caso, vengono in rilievo le disposizioni che disciplinano l'inadempimento contrattuale e la relativa responsabilità, le norme in materia di formazione del contratto e di manifestazione del consenso.

Si riscontra, invece, un preoccupante vuoto normativo in relazione in tema di protezione dei “consumatori” quali utilizzatori dei Bitcoin, aspetto che, secondo la dottrina, dovrebbe essere oggetto di particolari obblighi informativi, vista anche la tendenza delle comunicazioni in tema di “monete virtuali” emesse dalle autorità bancarie europee ad assumere la forma di “avvertenze” rivolte a questa tipologia di acquirenti, con la finalità di metterli in guardia rischi derivanti dall'assenza di regolamentazione.

In un'ottica volta ad offrire una forma di protezione ci si è interrogati sulla possibilità di estendere loro le garanzie offerte dalla legislazione in materia di sorveglianza bancaria e finanziaria, di trasparenza, nonché dei sistemi di garanzia obbligatoria dei “fondi” depositati. L'ostacolo giuridico all'estensione di queste norme è costituito dalla previsione quale presupposto della sua applicabilità “dell'esercizio dell'attività bancaria”, ritenuta assente rispetto al sistema di Bitcoin. Diversa potrebbe essere la situazione se e nella misura in cui si consolideranno le strutture delle poche “banche” di Bitcoin già esistenti, ed in particolare se queste inizieranno a concedere prestiti in Bitcoin.

Rispetto alla possibilità di sottoporre i Bitcoin alla disciplina bancaria, non sono mancate delle osservazioni critiche, volte a porre in evidenza il pericolo che tale normativa possa incidere negativamente sulla duttilità propria di queste monete virtuali, facendo venir meno alcuni degli elementi che li rendono particolarmente appetibili per gli acquirenti, come l'assenza di intermediari o di costi per le transazioni.

Infine, vengono ritenute applicabili ai Bitcoin anche le norme in materia di fallimenti e, in particolare, quelle che regolano quelli transfrontalieri.

3. Disciplina pubblicistica: trattamento fiscale e norme penali.

3.1. Profili di rilevanza penale delle criptovalute.

Le criptovalute costituiscono un'importante innovazione tecnologica, capace di incidere su diversi aspetti della vita degli individui, anche in modo negativo, favorendo la consumazione di alcuni reati.

Una delle ragioni del loro successo è il legame tra tecnologia e monete virtuali che, a seconda delle modalità di emissione, vengono distinte in criptovalute e token.

Alla base della loro creazione c'è la volontà di creare un sistema monetario alternativo a quello tradizionale, in grado di autoregolarsi, basato sulla fiducia reciproca tra gli operatori e su una tecnologia in grado di garantire l'unicità della transazione.

Come si vedrà nel prosieguo della lettura del presente articolo, caratteristiche come l'anonimità, l'utilizzo di alcuni escamotage (si pensi al c.d. *mixing*) sono in grado di rendere difficile risalire a tutte le transazioni compiute o all'origine della stessa catena di transazioni, grazie al mascheramento dell'indirizzo IP o all'utilizzo di browser di navigazione che garantiscono l'anonimato.

Vi sono, come emergerà dalla disamina che segue dei reati che più di altri si sono avvantaggiati di tali caratteristiche.

la criminalità è riuscita, infatti, a sfruttare a proprio vantaggio tutti quei meccanismi ideati al fine di garantire la privacy e la sicurezza degli utenti, per realizzare operazioni occulte e sottrarle a qualsiasi forma di controllo.

Una delle principali caratteristiche delle criptovalute e del Bitcoin che ne è la principale espressione è, infatti, l'anonimato, poiché i soggetti coinvolti vengono identificati solo attraverso una stringa alfanumerica che rende pressoché irrintracciabili o difficilmente rintracciabili i suddetti soggetti²⁵.

Nella circolazione delle monete virtuali non è, infatti, prevista la presenza o l'intervento di un'Autorità di controllo che svolga compiti simili a quelli adempiuti dalle banche che hanno l'obbligo di verificare l'identità dei propri clienti; tali controlli, benché siano stati previsti dalla normativa antiriciclaggio, svolgendosi online, sono facilmente eludibili ed i sistemi di tracciamento, con le poche informazioni disponibili, del tutto inefficaci, essendo, di fatto, noti solo la *transaction chain* (catena di transazioni) e gli *adress* degli utenti, che possono utilizzarne un numero illimitato, tra cui possono essere intercorsi degli scambi di valute, informazioni non sempre disponibili per tutte le criptovalute²⁶.

Ulteriori meccanismi per ottenere l'occultamento delle informazioni sono: le VPN, ossia l'utilizzo di una rete privata virtuale, che rende l'indirizzo IP non visibile neanche al ISP che,

²⁵ L. STURZO, *Bitcoin e riciclaggio 2.0* in *Diritto penale contemporaneo*, n. 5/2018, pag. 21.

²⁶ Monero, Dash, e Zcash crypto, ad esempio, tendono ad occultare le transazioni.

adottando una politica di “no-log”, non registra neanche le attività compiute dagli utenti o l'utilizzo del browser Tor.

Queste caratteristiche hanno attratto la criminalità che ha intravisto nel loro sfruttamento la possibilità di compiere delle attività illecite, di effettuare transazioni di denaro e ripulire quello proveniente da attività illegali.

Le attività di riciclaggio non sono, tuttavia, le uniche che hanno beneficiato e saputo sfruttare a proprio vantaggio le caratteristiche delle monete virtuali. I c.d. *marketplace* (sito/piattaforma internet) sono, infatti, diventati vere e proprie piazze di spaccio di merci il cui commercio è vietato (si pensi alla droga o alle armi) o luoghi di scambio e commercializzazione di prodotti/servizi grazie ai quali sottrarsi al fisco²⁷ o ricevere denaro per attività illecite (si pensi al *ransomware* o al *wannacry*) come i cyber attacchi che rendono inaccessibili i dati contenuti nel computer, che in tempi recenti (2018/2020) sono passati dal 23% al 67%²⁸ o i furti diretti nei confronti dei *exchangers* o dei *wallet providers* per sottrarre loro i dati necessari per accedere alle criptovalute.

I reati la cui commissione è stata indubbiamente e maggiormente agevolata sono quelli previste dagli artt. 648-*bis* – Riciclaggio, 648-*ter* - Impiego di denaro, beni o utilità di provenienza illecita e 648-*ter*-1 – Autoriciclaggio; le ragioni sono quelle esaminate nel paragrafo precedente e sono strettamente connesse alle caratteristiche delle criptovalute e alle loro modalità di funzionamento che tendono a garantire l'anonimato degli utenti e a rendere difficoltosa l'individuazione e localizzazione non solo degli utenti, ma delle stesse attività, rendendo più agevole la loro commissione in forme illegali.

Le caratteristiche specifiche delle monete virtuali si inseriscono, inoltre, in un contesto normativo non sempre caratterizzato da disposizioni ben tipizzate o da un sistema di controlli poco efficace, con inevitabili ricadute negative sul piano sanzionatorio²⁹.

Il reato previsto dall'art. 648-*bis* è stato reso a forma libera; per la sua commissione, infatti, il legislatore non si è limitato a fare riferimento alle condotte di sostituzione o trasferimento di “denaro beni o altre utilità provenienti da delitto”, ma ha previsto il compimento di altre operazioni idonee ad ostacolare “l'identificazione della loro provenienza delittuosa”. In questo modo, la fattispecie è stata resa più elastica e capace di adattarsi all'evoluzione della tecnologia e di “arricchirsi” di nuove modalità di esecuzione e, grazie all'inciso “in modo tale da ostacolare l'identificazione della loro provenienza delittuosa”, a pericolo concreto³⁰.

²⁷ G. ACCINNI, *Profili di rilevanza penale delle “criptovalute” (nella riforma della disciplina antiriciclaggio del 2017)* in *Archivio Penale* n. 1/2018, pag. 10.

²⁸ G. SBARAGLIA, *Guida al ransomware: cos'è, come si prende e come rimuoverlo*, in *cybersecurity360.it*.

²⁹ L. LA ROCCA, *La prevenzione del riciclaggio e del finanziamento del terrorismo nelle nuove forme di pagamento. Focus sulle valute virtuali*, in *Analisi Giuridica dell'economia*, 2015 n.1, pag. 209.

³⁰ G. FIANDACA, E. MUSCO, *Diritto penale. Parte speciale*, VII ed., Bologna, 2015.

Sofferamoci, a questo punto, sull'elemento oggettivo della fattispecie, ossia sui termini "denaro, beni o altre utilità" per determinare se l'impiego di criptovalute possa comportare o meno la realizzazione del reato in esame. Rispetto al primo termine, la dottrina³¹ ha manifestato dei dubbi, poiché le monete virtuali non sono riconosciute dallo Stato come moneta avente corso legale.

La riconducibilità delle criptovalute entro la nozione di "beni", invece, appare più semplice, poiché l'espressione viene ritenuta elastica e comprensiva sia di quelli materiali che immateriali; allo stesso modo, non vi sono difficoltà né dubbi circa la riconducibilità delle monete virtuali entro il concetto di "altre utilità"³². Queste osservazioni inducono a ritenere che il reato in esame possa certamente essere commesso mediante l'uso di criptovalute e con la conversione in valuta virtuale anche di ingenti somme di denaro di illecita provenienza.

Un discorso analogo a quello appena esposto vale anche per il reato descritto nell'art. 648-ter; l'impiego delle espressioni "attività economiche o finanziarie denaro, beni o altre utilità" appare, infatti, conferire alla norma una grande elasticità che consente di ricomprendere in esse anche attività svolte con l'impiego di criptovalute.

La terza fattispecie è quella descritta nell'art. 648-ter.1 – Autoriciclaggio; anche in questo caso, la norma sembra essere stata concepita in modo da ricomprendere il *cyberlaundering*³³ realizzato mediante l'impiego di criptovalute³⁴.

Rispetto a questa terza tipologia di reato è importante prestare attenzione al contesto in cui l'utilizzo di monete virtuali deve collocarsi; le condotte devono, infatti, realizzarsi nell'ambito di attività economiche, finanziarie, imprenditoriali o speculative. Anche in questo caso, è necessario soffermarsi sulle singole espressioni ed esaminarle al fine di stabilire se lo scambio o conversione di criptovaluta possa essere qualificata come attività economica, finanziaria, imprenditoriale o speculativa. La dottrina ritiene che lo scambio/conversione di criptovalute non configuri né una attività economica³⁵ né imprenditoriale, mentre è più probabile che possa concretizzarsi in un'attività di tipo speculativo o finanziario; pertanto, lo scambio o conversione di moneta virtuale può certamente presentare gli estremi del reato previsto dall'art. 648-ter.1³⁶.

Alcuni autori³⁷ ritengono che il bene tutelato dalla norma non sia l'ordine economico, ma la tracciabilità dei flussi finanziari, interesse sicuramente leso da chi, avvalendosi delle monete

³¹ Si veda A. ROSATO, *Profili penali delle criptovalute*, Pisa, 2021.

³² L. PICOTTI, *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio* in *Rivista trimestrale diritto penale economia*, n. 3-4/2018, pag. 608.

³³ S. MURARI, *Cyberlaundering*, Ed. Pearson, 2003.

³⁴ M. CROCE, *Cyberlaundering e valute virtuali. La lotta al riciclaggio nell'era della distributed economy*, in *Sistema penale*, 4/2021, pag. 127.

³⁵ F. ANTOLISEI, *Manuale di diritto penale. Parte speciale – I*. XVI ed., Milano 2016.

³⁶ A. GULLO, *Il delitto di autoriciclaggio al banco d prova della prassi: i primi (rassicuranti) chiarimenti della Cassazione in Diritto penale e processo*, n. 4/2017, pag. 482.

³⁷ Si veda L. STURZO, *Bitcoin e riciclaggio 2.0*, in *Diritto penale contemporaneo* n. 5/2018, pag. 25 ss.

virtuali e delle risorse tecnologie, compia delle operazioni in mercati virtuali destinate a rimanere occulte ai terzi.

Il *cyberlaundering* mediante criptovalute non ha solo dimostrato la propria idoneità ad integrare le tre fattispecie esaminate, ma anche la sua duttilità a realizzare reati presupposto e nuovi reati strumentali; rispetto ai primi, il più noto è il c.d. *phishing*,³⁸ ossia la truffa telematica, che si realizza attraverso l'invio di messaggi o email contenenti l'invito a fornire dati riservati al fine di risolvere un problema di registrazione o di altra natura. L'utente può essere facilmente ingannato e fornire incautamente i propri dati, poiché le comunicazioni sono artatamente costruite in modo da indurre in errore il destinatario e indurlo a credere che lo stesso sia stato inviato da un istituto o sito a cui si è realmente iscritto.

In alcuni casi, ai messaggi possono essere allegati dei file che l'utente è invitato ad aprire per visionarne il contenuto. Gli allegati possono contenere dei virus dormienti (*financial malware o trojan banking*) che si attivano allorché l'utente inserisca la *user id* o delle *password* di accesso fornendo ai mittenti le chiavi di accesso agli account di posta elettronica o di e-commerce. Queste condotte possono integrare dei reati presupposto³⁹ dei delitti di riciclaggio, ovvero di impiego od anche di autoriciclaggio. Dopo aver carpito e utilizzato abusivamente le credenziali d'accesso del servizio di *home banking* della vittima, viene effettuata una transazione indirizzata ad un terzo, il quale provvede con ulteriori trasferimenti a "ripulire" e quindi dissimulare la provenienza delittuosa dei proventi del phishing. Al *phisher*, infatti, si può ascrivere la responsabilità per il delitto di autoriciclaggio *ex art. 648-ter.1* nel caso in cui egli stesso effettui operazioni sulle somme derivanti dai reati commessi nell'attività di phishing o concorra con il terzo.

Accanto agli inediti reati presupposto, vi sono da considerare anche i nuovi reati strumentali. È il caso di utilizzo di *smart cards* contraffatte o alterate in precedenza per effettuare operazioni di "lavaggio" di denaro sporco. In questo caso, il delitto configurabile è quello di cui all'articolo 493-*ter* c.p., ritenuto strumentale rispetto a quello di riciclaggio. La condotta di indebito utilizzo delle *smart cards* è, infatti, punibile autonomamente rispetto a quella compiuta da chi si sia servito delle *smart cards* per compiere delle operazioni di riciclaggio.

Sono ritenuti reati strumentali anche: il furto di identità digitale (art. 494 c.p.), il reato di accesso abusivo a sistema informatico o telematico (art. 615-*ter* c.p.)

³⁸ R. FLOR, *Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, in *Rivista italiana di diritto e procedura penale*, 2007, n. 2-3, pag. 892

³⁹ Frodi informatiche, anche aggravate dal furto di identità digitale (*ex art. 640-ter*, comma 3, c.p.), truffe *ex art. 640* c.p., acquisizione e cessione illecite di password (*ex art. 615-quater* c.p.), accessi abusivi a sistemi informatici o telematici (*ex art. 615-ter*, c.p.) ed altri delitti simili.

3.2 Disciplina fiscale e reati tributari.

L'individuazione dell'esatta natura delle monete virtuali pur essendo difficoltosa, appare propedeutica ai fini del loro inquadramento dal punto di vista fiscale e per individuare quali reati possano configurarsi. Come vedremo la difficoltà di individuare l'esatta natura delle criptovalute deriva principalmente dal tentativo di assimilarle a entità già note di cui, però, non hanno tutte le caratteristiche.

Di seguito esaminerò le soluzioni proposte, partendo da quella dell'Agenzia delle Entrate che, con la Risoluzione 9 settembre 2016, n. 72/E, ha affrontato il problema dell'inquadramento nell'ordinamento tributario delle operazioni di compravendita di valute elettroniche.

Nella Risoluzione, viene richiamata la pronuncia della Corte di giustizia del 22 ottobre 2015, C-264/2014 in base alla quale «Le operazioni che consistono nel cambio di valuta tradizionale contro unità della valuta virtuale “bitcoin” e viceversa, effettuate a fronte del pagamento di un “margine” costituito dalla differenza tra il prezzo di acquisto e quello di vendita, costituiscono prestazioni di servizi a titolo oneroso esenti da IVA in quanto riconducibili al dettato dell'art. 135, paragrafo 1, lettera e), della Direttiva IVA(direttiva 2006/112/CE)»⁴⁰.

L'Agenzia delle Entrate, ispirandosi a tale pronuncia ha, allo stesso modo, qualificato l'operazione come “prestazione di servizi di natura finanziaria” e l'ha ritenuta esente dall'imposta sul valore aggiunto ai sensi dell'art. 10, comma 1, n. 3), D.P.R. n. 633/1972, in quanto rientrante tra le «operazioni relative a valute estere aventi corso legale e a crediti in valute estere, eccettuati i biglietti e le monete da collezione e comprese le operazioni di copertura dei rischi di cambio»; alla luce di questa disposizione ci si chiede se i *wallet* delle criptovalute possano essere assimilati ad un conto deposito o conto corrente e se l'accostamento alle valute estere comporti, ai fini fiscali, l'obbligo della compilazione del quadro RW della dichiarazione dei redditi. La risposta a quest'ultimo interrogativo si rinviene nella risposta all'interpello n. 788 del 24 novembre 2021, in cui l'Agenzia ha precisato che le criptovalute devono essere indicate nel quadro RW anche se sono inserite in un *wallet* con chiave privata. L'obbligo viene assolto inserendo nella colonna 3 il codice 14 (altre attività estere di natura finanziaria e valute virtuali), mentre non è necessario compilare la colonna 4; l'obbligo riguarda tutte le valute virtuali detenute⁴¹.

Nella compilazione del quadro RW il controvalore in euro della moneta virtuale detenuta deve essere determinato al cambio indicato sul sito in cui la criptovaluta sia stata acquistata; la data di riferimento è quella del 31 dicembre dell'anno di riferimento.

⁴⁰ Corte giustizia UE sez. V, 22 ottobre 2015, n.264, in *Iltributario.it*, fasc., 22 dicembre 2015, con nota di S. MAZZOCCHI, *Esenti da IVA le operazioni di cambio nella valuta virtuale “bitcoin”*; si veda anche I. L. NOCERA, *Il cambio di valuta tradizionale contro valuta virtuale «bitcoin» è esente da IVA*, in *Diritto & Giustizia*, fasc. 39, 2015, pag. 11.

⁴¹ Nello stesso senso TAR Lazio, 27 gennaio 2020, n. 1077.

Nella stessa risposta, l’Agenzia ha anche chiarito che le valute virtuali non sono soggette all’imposta sul valore delle attività finanziarie detenute all’estero (IVAFE) dalle persone fisiche che risiedano nel territorio dello Stato⁴², essendo tale imposta applicata solo ai depositi e conti correnti di natura bancari; implicitamente, quindi, l’Agenzia ha escluso che i *wallet* possano ritenersi tali.

Non essendo i suddetti redditi soggetti a imposizione, vengono meno i requisiti necessari per considerare l’applicazione dei reati enunciati nel d.lgs. 74/2000 agli art. 4, 5 e 10-ter (rubricati rispettivamente Dichiarazione infedele, Omessa dichiarazione e Omesso versamento di IVA).

Nell’effettuare la propria disamina delle questioni fiscali afferenti alle operazioni compiute con valute virtuali, l’Agenzia delle Entrate, ha ritenuto di dover discernere i profitti degli operatori professionali relativi alla conversione di criptovalute (gli *exchange*), dai profitti delle persone fisiche che detengono criptovalute (e che compiano operazioni di acquisto e alienazione delle stesse).

Ai fini dell’imposizione diretta, la differenza tra il prezzo di acquisto e quello di vendita costituisce componente positiva o negativa rientrante nell’attività caratteristica di intermediazione e pertanto concorre alla formazione della base imponibile IRES (o IRPEF) e IRAP. Ritenendo che i redditi degli *exchanger*, derivanti dall’attività di intermediazione contribuiscono alla «formazione della base imponibile soggetta ad ordinaria tassazione ai fini IRES», l’Agenzia ha ritenuto configurabili i reati ascritti agli artt. 2 e 3 d.lgs. 74/2000 (dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti e Dichiarazione fraudolenta mediante altri artifici) e i reati agli artt. 4 e 5 d.lgs. 74/2000, in caso di superamento delle soglie di punibilità⁴³.

Per stabilire il valore delle criptovalute che restino nella disponibilità dell’acquirente-venditore al termine dell’esercizio deve farsi riferimento al valore del cambio, indicato sulle piattaforme on-line in cui avvengono le compravendite di Bitcoin, al momento della conclusione dell’esercizio stesso.

Per i c.d. *miners* (minatori) per determinare il regime fiscale dei bit ottenuti come ricompensa deve tenersi conto se abbiano organizzato le risorse necessarie alla loro “produzione”, in questo caso i relativi profitti rientrano nel reddito di impresa abituale (art. 55 TUIR) o se si sia trattato di un’attività di impresa occasionale, i cui redditi vengono inclusi tra i redditi diversi (art. 67 TUIR)⁴⁴.

⁴² T. GAVI, *Criptovalute e dichiarazione dei redditi: si devono indicare nel quadro RW*, in *informazioneefiscale.it*.

⁴³ R. LUCEV, F. BONCOMPAGNI, *Criptovalute e profili di rischio penale nelle attività degli exchanger*, in *Giurisprudenza penale* n. 3/2018.

⁴⁴ Dai primi è possibile dedurre i costi di produzione, i secondi invece vengono sottoposti a tassazione al lordo dei costi sostenuti

Rispetto al cliente, invece, non rinvenendosi un'attività di impresa o professionale, né speculativa, non si determina alcuna base imponibile ai fini delle imposte sui redditi, impedendo che possa trovare applicazione l'art. 67 TUIR, relativo ai redditi diversi.

L'*exchanger*, a sua volta, non sarà sanzionabile né *ex art. 5*, comma 1-*bis* d.lgs. 74/2000 (Omessa dichiarazione del sostituto d'imposta), non essendo questi tenuto ad alcun adempimento quale sostituto d'imposta, né per i reati di omesso versamento, *ex art 10-bis e 10-ter*, d.lgs. 74/2000.

Pertanto le criptovalute e le attività svolte avvalendosi di esse possono essere dirette protagoniste dei reati di riciclaggio e, allorché configurino delle attività professionali, anche di tipo tributario.

4. Bitcoin e Blockchain Technology.

La Blockchain può essere considerata una delle innovazioni tecnologiche più controverse e dibattute dato che rappresenta uno nuovo strumento in grado di modificare radicalmente gli schemi di organizzazione sociale, economica e politica⁴⁵.

Questo nuovo strumento della tecnologia si sviluppa in seguito allo scalpore che generarono la diffusione dei Bitcoin, e cioè di un rivoluzionario sistema di pagamento online privo di qualsiasi ente centrale che ha letteralmente scombussolato l'intero mondo della finanza creando il cosiddetto mito della intermediazione⁴⁶.

È facile far coincidere la nascita della tecnologia Blockchain con l'avvento dei Bitcoin in quanto quest'ultimi ne rappresentano la prima effettiva applicazione.

Lo sviluppo della tecnologia Blockchain coincide, nel 2008, con la pubblicazione da parte di un misterioso Satoshi Nakamoto⁴⁷ di un paper dal titolo "*Bitcoin: A Peer-to-Peer Electronic Cash System*", nel quale viene dettagliatamente illustrata il funzionamento di tale tecnologia⁴⁸.

La Blockchain, quindi, nasce avendo come obiettivo la realizzazione di un progetto definito e cioè quello di creare un sistema di pagamento virtuale assolutamente indipendente dalle istituzioni.

Tuttavia, per comprendere su quali basi si struttura questa nuova tecnologia è necessario dedicare qualche cenno al cosiddetto movimento del *Cyberpunk* sorto, nei primi anni novanta, per

⁴⁵ E. FAGLIA, *Blockchain e smart contract: un inquadramento tra profili tecnici e giuridici*, in *Trento Law and Technology Research Group Student Paper*, 2019, n. 51, pag. 3 ss.

⁴⁶ Cfr. D. TAPSCOTT, A. TAPSCOTT, *Blockchain Revolution: How the Technology Behind Bitcoin and Others Cryptocurrencies is Changing the World*, Penguin Books Ltd, 2016; F. BOUCHER, S. NASCIMENTO, M. KRITIKOS, *Come la tecnologia blockchain può cambiarci la vita*, Servizio Ricerca del Parlamento Europeo, 2017.

⁴⁷ Identità di Satoshi Nakamoto è, tutt'ora, sconosciuta. Potrebbe trattarsi di una persona, così come di un gruppo di persone.

⁴⁸ Curiosamente, il paper di Satoshi Nakamoto non contiene il termine "*Blockchain*", ma solo l'espressione "chain of blocks". La parola Blockchain ha cominciato a diffondersi in Rete successivamente al lancio di Bitcoin.

iniziativa di Eric Hughes, Tim Way e Jhon Gilmore che creano una mailing list sulla quale si discute dei temi della privacy e della cifratura dei dati. A conclusione del loro lavoro pubblicano il manifesto⁴⁹ del movimento con lo scopo di diffondere l'utilizzo della crittografia: che avrebbe avuto come obiettivo primario quello di facilitare la contrattazione privata, la libertà individuale e smantellare, di fatto, lo stato-nazione⁵⁰.

Secondo May, uno dei partecipanti al Manifesto appena menzionato, lo scopo del lavoro promosso dal gruppo al quale appartiene è quello di sollecitare il popolo della rete all'utilizzo della crittografia che, a suo parere, è l'unico strumento che garantirebbe la libertà dei cittadini in modo da difendersi dal controllo che i governi nazionali che, spesso proprio attraverso il monitoraggio dei dati scambiati in rete, sono in grado di limitare e condizionarne le scelte degli individui.

Già alla fine degli anni ottanta May mette in guardia i cittadini sostenendo che lo Stato avrebbe continuato ad osteggiare vivacemente la diffusione di questa nuova tecnologia motivando tale ammonimento in ragione di questioni di sicurezza nazionale⁵¹.

In realtà May, in largo anticipo, sarà il sostenitore dell'importanza di assicurare l'anonimato nelle transazioni che si sviluppano all'interno delle reti telematiche principio, questo, che, nel 2008, culminerà nella creazione di Bitcoin.⁵²

Anche se dal 2008 ad oggi il panorama inizialmente ideato da May, che rappresenta il punto di partenza per lo sviluppo della crittografia digitale, è cambiato radicalmente, e con riguardo alla

⁴⁹ E. HUGHES, *A Chypherpunk's Manifesto*, 9 marzo 1993.

⁵⁰ *Ivi*.

⁵¹ Cfr. T.C. MAY, *The Crypto Anarchist Manifesto*, Satoshi Nakamoto Institute, ove è possibile leggere che «...lo stato continuerà naturalmente a provare a rallentare o fermare la diffusione di questa tecnologia, adducendo questioni di sicurezza pubblica nazionale, rischi di utilizzo della tecnologia da parte di spacciatori ed evasori, e timori di disintegrazione sociale. Molte di queste motivazioni saranno valide; la cripto-anarchia permetterà ai segreti di stato, così come a materiali illeciti e rubati, di essere scambiati liberamente. Un mercato anonimo computerizzato renderà addirittura possibili ripugnanti mercati per assassini e estorsioni. Diversi elementi criminali e stranieri saranno utenti attivi della CryptoNet. Ma questo non fermerà la diffusione della cripto-anarchia».

⁵² Bitcoin non è stato il primo tentativo di creare un sistema di pagamento online indipendente dalle istituzioni. Al contrario, esso può considerarsi "l'ultima" tappa di un percorso, durato poco più di un decennio, in cui ve-dono la luce una serie di innovazioni tecnologiche senza le quali né Bitcoin né la Blockchain sarebbero mai potute venire ad esistenza. Si segnala, in particolare, il servizio B-Money, proposto nel 1998 da Wei Dai, consistente in un sistema decentralizzato di pagamento garantito dalla crittografia e dalla c.d. "Proof of Stake" (un meccanismo finalizzato ad incentivare i partecipanti ad agire onestamente nel network, pena la perdita dei fondi depositati). Nonostante l'assenza di controllo governativo, la proposta B-Money di Wei Dai assicura che tutte le transazioni siano verificate da una rete decentralizzata, che mantiene altresì un registro permanente e ufficiale. Il registro non simboleggia valore posseduto in qualche altra forma, ma costituisce effettivamente, esso stesso, quel valore. Inoltre, "nuova" b-money viene generata – essenzialmente, coniata – attraverso l'utilizzo del potere computazionale necessario per risolvere le sfide crittografiche richieste dal protocollo. Oltre a B-Money, fondamentale importanza rivestono il meccanismo Proof of Work, teorizzato nel 2004 da Hal Finney e successivamente utilizzato dalla stessa Bitcoin, ed il servizio Bitgold proposto da Nick Szabo nel 2005, che presenta molte delle caratteristiche che appariranno tre anni più tardi in Bitcoin. Per una più approfondita disamina degli sviluppi tecnologici che hanno consentito la nascita di Bitcoin, della Blockchain e dello Smart Contract v. M. NICOTRA, F. SARZANA DI SANT'IPPOLITO, *Diritto della blockchain, intelligenza artificiale e IoT*, Padova, 2018, p. 9 ss. e p. 90 ss.; J. GOLDENFEIN, D. HUNTER, *Blockchains, A technical History of Bitcoin and Blockchains*, in *Orphan Works*, cit., p. 5 ss.

tecnologia Blockchain sono state sviluppate una serie di eterogenee applicazioni e protocolli informatici.

La dottrina, tuttavia, ha fornito una definizione alla Blockchain affermando che la stessa può essere definita come una struttura matematica che consente di memorizzare dati in un modo tale da rendere impossibile qualsiasi modifica⁵³.

Stando alla definizione comunemente accettata la Blockchain consiste in una tecnologia che sfrutta un registro digitale distribuito fra i partecipanti, sul quale è riportata una catena di blocchi di dati legati da principi crittografici gli uni agli altri. Attraverso tale sistema gli utenti si scambiano asset digitali e registrano informazioni senza la necessità di ricorrere ad un ente centrale che eserciti funzioni da controllo e di garanzia.⁵⁴

Occorre precisare, tuttavia, che la tecnologia Blockchain rientra nella più ampia categoria di DLT (Distributed Ledger Technology) o tecnologie di registro distribuito e disintermediato, l'elemento che differenzia una Blockchain rispetto da un DLT è costituito dalla struttura a blocchi di registro che caratterizza la prima; tranne che per questo elemento distintivo spesso i termini di Blockchain e DLT vengono utilizzati come sinonimi⁵⁵.

Ma vediamo ora come funziona, in concreto, la Blockchain.

Attraverso tale tecnologia è possibile scambiare valori verificati, approvati e certificati in rete avvalendosi di un registro digitale distribuito ai partecipanti sul quale viene riportata una catena di blocchi di dati legati da principi crittografici.

Una delle caratteristiche della Blockchain coincide, quindi, con un network di utenti ognuno dei quali detiene una copia aggiornata del registro sul quale vengono iscritte le varie transazioni.

La gestione del registro non è rimessa ad un ente centrale, bensì ad una rete di soggetti che, in modo democratico, sono in grado di decidere quali informazioni vanno registrate raggiungendo il consenso. Proprio il funzionamento del meccanismo del consenso varia a seconda di come lo stesso viene progettato in ogni singola Blockchain: e quindi può essere aperto alla partecipazione di tutti, oppure possono prendervi parte solo soggetti che soddisfino determinate condizioni⁵⁶.

Altro elemento che caratterizza la Blockchain è l'utilizzo della crittografia. Il registro di una Blockchain, infatti, è composto da blocchi di dati che sono crittograficamente collegati l'uno

⁵³ M. SIENA, *La tecnologia Blockchain: criticità dal punto di vista legale, prime applicazioni e prospettive*, in *LLR*, 2019, 1, pag. 49 ss.

⁵⁴ Tecnicamente la Blockchain va identificata come la tecnologia che sfrutta un registro distribuito così come illustrato nel testo. Tuttavia, spesso il termine Blockchain viene utilizzato per indicare il registro distribuito stesso. È questo il caso, per esempio, quando si parla di “dati registrati sulla Blockchain”. Nel corso dell’elaborato il termine verrà utilizzato in ambedue i sensi ed il contesto renderà chiaro in quale significato la parola è intesa.

⁵⁵ V. LEMMA, *Quali controlli per le valute virtuali?* in *Riv. Trim. di diritto dell’economia*, suppl. n. 3 al n.1/2022, pag. 53 ss.

⁵⁶ Per una panoramica dei principali meccanismi di consenso attualmente utilizzati si vedano P. KRAVCHENKO, *Consensus explained*, Medium, 2017; M. NICOTRA, F. SARZANA DI SANT’IPPOLITO, *ult.op.cit.*, pag. 26 ss.

all'altro in modo da formare una catena di blocchi (che ne giustifica quindi il nome block-chain): ogni blocco contiene una marca temporale in modo che la catena di blocchi segua un ordine cronologico⁵⁷.

Dal collegamento crittografico fra di loro dei vari blocchi di dati implica che ogni blocco sia legato al precedente determinando come effetto il fatto che l'eventuale manomissione di un blocco produrrebbe effetti sul blocco successivo, interrompendo di fatto la catena che sarebbe automaticamente conosciuta da tutti i partecipanti.⁵⁸

La tecnologia Blockchain, quindi consente la creazione di un nuovo e rivoluzionario modello per consentire gli scambi nelle reti, o meglio per consentire gli scambi fra quei soggetti che si sono riconosciuti ed operano nelle reti.

Nelle Blockchain è possibile individuare le organizzazioni decentralizzate (DO) e le organizzazioni autonome decentralizzate (DAO) che rappresentano una sottocategoria delle applicazioni decentralizzate (DApps)⁵⁹.

La fonte principale di disciplina delle organizzazioni decentralizzate DO coincide con l'autodisciplina della tecnologia blockchain. Le organizzazioni decentralizzate permettono agli individui di cooperare e di effettuare transazioni, da un nodo all'altro, senza la necessità di ricorrere ad un intermediario convenzionale.

Secondo la dottrina⁶⁰, quindi, in futuro le piattaforme che intervengono nelle relazioni fra i partecipanti possano essere sostituite dalle piattaforme create da una organizzazione decentralizzata DO; da tale eventualità scaturirebbe la possibilità di creare un'associazione cooperativa che potrebbe essere gestita dal lato dell'offerta, in questo modo i partecipanti possono dividere fra di loro i profitti senza veder destinata alcuna quota agli intermediari.

Per quanto concerne, invece, il controllo umano questo è decisamente limitato nell'ambito di un'organizzazione autonoma decentralizzata (DAO).

La DAO, quindi, non fa altro che esprimere una relazione reciproca che viene ad instaurarsi fra individui, aziende e macchine in modo da creare «un ecosistema complesso di agenti autonomi che in interagiscono tra loro secondo un insieme di regole predeterminate, cablate e auto-imponenti»⁶¹. In base a tale organizzazione gli esseri umani scelgono di interagire fra di loro nel rispetto di un protocollo previsto dal codice informatico che viene poi applicato nella rete della blockchain.

⁵⁷ V. LEMMA, *Quali controlli per le valute virtuali?* op. cit., pag. 53 ss.

⁵⁸ Per una più dettagliata illustrazione circa la conformazione di ciascun singolo "blocco", si M. NICOTRA, F. SARZANA DI SANT'IPPOLITO, op. cit., p. 13.

⁵⁹ C. PONCIBÒ, *Il diritto comparato e la Blockchain*, Napoli, 2020, pag. 83 ss.

⁶⁰ V. LEMMA, *Quali controlli per le valute virtuali?* op. cit., pag. 53 ss.

⁶¹ A. WRIGHT, P. DE FILIPPI, *Decentralized Blockchain Technology and The Rise of Lex Cryptographia*, working paper, 2015.

In pratica, quindi, attraverso la creazione di una DAO (Organizzazione autonoma decentrata) viene a crearsi un soggetto che è in grado di gestirsi autonomamente attraverso la tecnologia che dovrebbe creare una sorta di autoregolamentazione non richiedendo, per l'esercizio di funzioni di amministrazione e di controllo, la delegazione del relativo potere ad un organo amministrativo.

Quindi questo in altri termini comporta che la creazione di un'organizzazione autonoma decentrata determina che la stessa non sia amministrata in virtù di delibere assunte da un'organizzazione centralizzata, ma sulla base di uno *smart contract* che spesso viene guidato dai detentori dei token che, pur non assumendo cariche manageriali, sono dotati di pieni poteri di gestione di tale organizzazione⁶².

4.1. La Blockchain: la necessità di colmare il vuoto normativo.

Dopo aver evidenziato gli aspetti prettamente tecnici della tecnologia blockchain è necessario dedicare qualche cenno ai profili giuridici del fenomeno, soffermandosi tanto sull'impulso della normativa europea, quanto sull'attenzione riservata dalla disciplina nazionale⁶³.

Proprio l'Unione Europea ha riservato alla tecnologia Blockchain grande attenzione tanto da adottare una serie di importanti iniziative fra le quali, tra le prime, figura la Risoluzione del 3 ottobre 2018 “*Sulle tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione*”.

Questa risoluzione riconosce la portata innovativa di tale tecnologia puntualizzando come la stessa sia «in grado di migliorare l'efficienza dei costi delle transazioni, ridisegnando anche le catene del valore e migliorando l'efficienza organizzativa attraverso un decentramento affidabile».

Il Parlamento europeo, inoltre, sempre attraverso tale risoluzione ha ribadito che la tecnologia blockchain può rafforzare l'autonomia dei cittadini eliminando i costi dell'intermediazioni nelle transazioni ed aumentandone la trasparenza⁶⁴.

Il Parlamento europeo, tuttavia, non ignora allo stesso tempo i pericoli connessi all'utilizzo di tali tecnologie, evidenziando con solerzia e precisione che gli innumerevoli rischi e problemi ad esse connessi non sono ancora completamente noti e che, anche il ricorso a tecnologie come quella

⁶² Per una definizione dell'espressione token, vedasi C. PONCIBÒ, *op.cit.*, pag. 90 ss, ove puntualizza che ci si riferisce al processo di cartolarizzazione (o comunque ad un processo molto simile in pratica) dei diritti su alcune tipologie di beni materiali o di beni immateriali che prende il nome, fra i tecnici, di «tokenizzazione». Un bene mobile o immobile può essere oggetto di siffatto processo di cartolarizzazione ed essere rappresentato digitalmente sotto forma di token. Lo scambio di token ha luogo fra i nodi senza alcun limite legale o territoriale.

⁶³ F. FAINI, *Blockchain e diritto: la “catena del valore” tra documenti informatici, smart contracts e data protection*, in *Resp. civ. e prev.*, 1° gennaio 2020, fasc. 1, pag. 297 ss.

⁶⁴ C. PONCIBÒ, *op.cit.* pag. 149 ss.

della blockchain richiede sempre l'osservanza di tali irrinunciabili garanzie: la certezza del diritto, la tutela dei consumatori degli investitori e dell'ambiente⁶⁵.

Secondo la valutazione del Parlamento europeo è indispensabile garantire un adeguamento del quadro giuridico normativo alle innumerevoli novità che ormai comporta la diffusione di prodotti e nuove tecnologie connesse all'utilizzo della rete.

Fra l'altro la dottrina ha evidenziato come quella che ha investito il web può essere considerata come una vera e propria rivoluzione: caratterizzata da un enorme sviluppo della rete internet che ha permesso la nascita di un fenomeno in costante crescita ossia quello del commercio elettronico che ha richiesto addirittura l'intervento della Direttiva⁶⁶ 2000/31/CE (Direttiva sull'E-Commerce).

Uno dei principi più importanti stabiliti da tale Direttiva è previsto dal considerando numero 5: ove viene richiesto agli Stati membri di evitare differenze legislative nell'ambito della disciplina della cosiddetta società dell'informazione e del commercio elettronico anche tenendo conto delle caratteristiche transfrontaliere del fenomeno.

In tema di blockchain due sono i passaggi di cui tener conto in ambito europeo e cioè: l'istituzione da parte della Commissione europea dell'EU *Blockchain Observatory and Forum* il 1° febbraio 2018 e dell'*European Blockchain Partnership* del 10 aprile 2018.

Per quanto concerne il *Blockchain Observatory and Forum* è stato attribuito il compito di raccogliere tutte le informazioni esistenti in modo da garantire un approccio al fenomeno uniforme e comune in tutti i paesi europei⁶⁷.

Per quanto riguarda invece l'*European Blockchain Partnership* questa è protesa a consolidare il ruolo dell'Europa nella diffusione della tecnologia blockchain individuando una disciplina uniforme in Europa.

Tra le iniziative promosse figura anche quella diretta alla creazione di una *European Blockchain Services Infrastructure (ESB)* che garantisce la fornitura di servizi pubblici transfrontalieri in tutta l'Europa: utilizzando la tecnologia blockchain garantendo alti standard di sicurezza e protezione dei dati personali⁶⁸.

⁶⁵ F. FAINI, *op.cit.*, pag. 300 ss.

⁶⁶ Dir. 08/06/2000, n. 2000/31/CE Direttiva del Parlamento europeo e del Consiglio relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("Direttiva sul commercio elettronico").

⁶⁷ Sono particolarmente interessanti i report tematici prodotti dall'Osservatorio, che affrontano anche le sfide giuridiche poste da tale tecnologia: ai fini di tale analisi, v. il report *Legal and regulatory framework of blockchains and smart contracts*, pubblicato il 27 settembre 2019; e il report *Blockchain and the GDPR*, pubblicato il 16 ottobre 2018; cfr. <https://www.eublockchainforum.eu/eu-blockchain-observatory-forum>. Al riguardo, a livello europeo riveste particolare interesse, altresì, il report *Blockchain for digital government. An assessment of pioneering implementations in public services* del Joint Research Centre (JRC), pubblicato il 23 aprile 2019.

⁶⁸ L'European Blockchain Services Infrastructure (EBSI) prenderà forma come una rete di nodi distribuiti in tutta Europa e diventerà un Building Block del Connecting Europe Facility (CEF), fornendo software, specifiche e

Recentemente, sempre a livello europeo, il Regolamento MiCA (*Markets in Crypto-Assets Regulation*), o Regolamento (UE) 2023/1114, è la normativa europea che crea un quadro normativo armonizzato per le cripto-attività e i relativi fornitori di servizi, con l'obiettivo di tutelare gli investitori, garantire la stabilità finanziaria e promuovere l'innovazione. Tra gli obiettivi principali vi è l'armonizzazione: creare un insieme di regole uniche e omogenee per l'intero mercato europeo delle cripto-attività, superando la frammentazione normativa tra gli Stati membri; la tutela dei consumatori e investitori, ossia proteggere gli utenti finali da rischi come le manipolazioni di mercato e le frodi, imponendo requisiti di trasparenza e obblighi di vigilanza; la stabilità finanziaria per prevenire abusi, come quelli legati a insider trading e manipolazione del mercato, e garantire la stabilità del sistema finanziario.

Spostando l'indagine alla disciplina nazionale invece bisogna tener conto prima dall'articolo 8-ter⁶⁹ del decreto-legge 135/2018, convertito in legge 12/2019 che disciplina tecnologie basate su registri distribuiti riservando ampia applicazione agli *smart contracts*, demandando allo stesso tempo la predisposizione di linee guida per determinarne le regole tecniche all'Agenzia per l'Italia digitale⁷⁰.

Malgrado le norme appena citate figurano senza alcun dubbio nell'alveo della disciplina dell'innovazione tecnologica, il legislatore ha incomprensibilmente scelto di non far confluire le stesse all'interno del testo del decreto legislativo 82/2005 noto come Codice dell'amministrazione digitale (CAD).

Da ultimo, per recepire il Regolamento MiCA (*Markets in Crypto-Assets Regulation*), o Regolamento (UE) 2023/1114, a livello nazionale le disposizioni relative alle criptovalute sono contenute nella Legge di Bilancio 2023, ossia nella l. n. 197/2022.

servizi riutilizzabili per supportarne l'adozione da parte delle istituzioni dell'Unione Europea e delle Pubbliche Amministrazioni europee.

⁶⁹ L'art. 8-ter. "Tecnologie basate su registri distribuiti e smart contract"¹. Si definiscono «tecnologie basate su registri distribuiti» le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetture decentralizzate su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili.² Si definisce «*smart contract*» un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse. Gli *smart contract* soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con linee guida da adottare entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto.³ La memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui all'articolo 41 del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014.⁴ Entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto, l'Agenzia per l'Italia digitale individua gli standard tecnici che le tecnologie basate su registri distribuiti debbono possedere ai fini della produzione degli effetti di cui al comma 3.

⁷⁰ Sull'analisi della norma cfr. C. BOMPRESZI, *Commento in materia di Blockchain e Smart contract alla luce del nuovo Decreto Semplificazioni*, in *Dir. merc. tecn.*, 2019, 1-7; F. SARZANA DI SANT'IPPOLITO, *Blockchain e smart contract nel nuovo decreto semplificazioni*, in *Dir. Internet*, 2019, 17-23.

Prima dell'introduzione del regolamento MiCA, il panorama normativo europeo in materia di crypto-attività risultava fortemente frammentato. Alcune di queste attività, in particolare quelle rientranti nella categoria di strumenti finanziari secondo la direttiva 2014/65/UE del Parlamento Europeo e del Consiglio, erano già regolate dalla legislazione dell'Unione sui servizi finanziari. Per tali crypto-attività esisteva un quadro normativo esaustivo, che disciplinava sia gli emittenti sia le imprese coinvolte, garantendo così un sistema chiaro e strutturato. Tuttavia, molte altre tipologie di crypto-attività non trovavano spazio nella normativa europea vigente in materia di servizi finanziari, come stabilito dalla Direttiva 2014/65/UE (MiFID II) e dal Regolamento (UE) n. 600/2014 (MiFIR). Tranne che per gli obblighi previsti dalla normativa antiriciclaggio (Direttiva (UE) 2015/849, AMLD), non esistevano regole specifiche che disciplinassero i servizi correlati a queste crypto-attività. Di conseguenza, risultavano scoperti aspetti fondamentali quali il funzionamento delle piattaforme di trading (escluse da MiFID II), lo scambio di crypto-attività con valuta fiat o altre crypto-attività, nonché i servizi di custodia e amministrazione delle stesse per conto dei clienti. Questa mancanza di un inquadramento normativo chiaro esponeva i titolari di crypto-attività a rischi significativi, soprattutto in settori non tutelati dalle norme sulla protezione dei consumatori sancite dalla Direttiva 2011/83/UE. Si creavano anche rischi per l'integrità del mercato, come abusi di mercato (Regolamento (UE) n. 596/2014) e crimini finanziari. Per mitigare tali problematiche, alcuni Stati membri avevano escogitato regolamentazioni ad hoc per gestire le crypto-attività non coperte dalla legislazione europea sui servizi finanziari, mentre altri avevano scelto di intraprendere iniziative normative autonome. L'assenza di un quadro comune e armonizzato a livello europeo indeboliva la fiducia degli utenti nelle crypto-attività, ostacolando lo sviluppo di un mercato unico per queste tecnologie. Questo vuoto legislativo si traduceva inoltre in una perdita di opportunità nell'ambito dei servizi digitali innovativi, degli strumenti alternativi di pagamento e delle nuove possibilità di finanziamento per le imprese dell'UE. Le aziende che utilizzavano crypto-attività operavano senza una chiara certezza giuridica sulle normative applicabili nei diversi Stati membri, limitandone la capacità di innovare e competere. Inoltre, un ritardo prolungato nell'introduzione di regole uniformi avrebbe potuto aggravare la frammentazione normativa tra i vari Paesi, generando distorsioni della concorrenza nel mercato unico europeo e complicando l'espansione transfrontaliera dei fornitori di servizi legati alle crypto-attività. Parallelamente, sarebbe aumentato il rischio di fenomeni di arbitraggio normativo tra le diverse giurisdizioni dell'Unione.

Il legislatore europeo attribuisce un ruolo centrale alla cooperazione con organismi internazionali come il Consiglio per la Stabilità Finanziaria, il Comitato di Basilea per la Vigilanza Bancaria e il Gruppo di Azione Finanziaria Internazionale per la regolamentazione delle crypto-attività. Tale approccio è essenziale per garantire l'allineamento delle normative dell'Unione alle migliori pratiche globali, prevenire l'arbitraggio normativo e promuovere una supervisione

efficace, contribuendo così alla stabilità finanziaria internazionale. La collaborazione con questi organismi consente inoltre di armonizzare le regolamentazioni e affrontare in modo coordinato le sfide globali imposte dalle cripto-attività, rafforzando integrità e stabilità nei mercati finanziari globali. Un secondo principio cardine della normativa è il rispetto del principio “stessa attività, stessi rischi, stesse norme” e della neutralità tecnologica nell’ambito dei servizi finanziari dell’Unione. Le cripto-attività che rientrano nel perimetro legislativo esistente continueranno quindi a essere regolate dal quadro attuale, senza distinzione per la tecnologia utilizzata nella loro emissione o trasferimento. Il regolamento MiCA esclude esplicitamente alcune categorie di cripto-attività già coperte da altre normative. Tra queste vi sono le cripto-attività classificate come strumenti finanziari ai sensi della Direttiva 2014/65/UE (MiFID II), nonché quelle definite depositi dalla Direttiva 2014/49/UE, inclusi i depositi strutturati. Anche i token di moneta elettronica, che pur presentano somiglianze con i depositi, non rientrano in questa categoria secondo la Direttiva 2009/110/CE. Sono escluse inoltre cripto-attività che si qualificano come fondi in base alla Direttiva (UE) 2015/2366 (PSD2), a meno che non siano token di moneta elettronica. Altri ambiti esclusi comprendono le cripto-attività che rappresentano posizioni verso cartolarizzazioni definite nel Regolamento (UE) 2017/2402, i contratti assicurativi, i prodotti pensionistici e i regimi di sicurezza sociale. Anche le cripto-attività considerate uniche e non fungibili, quali arte digitale e collezionabili, sono escluse dal regolamento per via della loro specificità. Tuttavia, nel caso in cui tali cripto-attività siano emesse in serie o siano di fatto fungibili, potrebbero rientrare nelle disposizioni normative del MiCA. Sono esonerate altresì le operazioni infragruppo e le attività svolte da enti pubblici quali il Fondo Monetario Internazionale o la Banca dei Regolamenti Internazionali, laddove non sussistano rischi rilevanti per la stabilità finanziaria. Le valute digitali emesse dalle banche centrali o da autorità pubbliche sono ugualmente escluse dal regolamento sul mercato delle cripto-attività. Al fine di tracciare una linea chiara tra cripto-attività regolate e strumenti finanziari, l’ESMA ha il compito di fornire orientamenti sui criteri necessari per qualificare le cripto-attività come strumenti finanziari. Questi criteri devono anche determinare le circostanze in cui cripto-attività apparentemente uniche potrebbero essere considerate strumenti finanziari fungibili. Per garantire un approccio coerente nella classificazione delle cripto-attività, l’ABE, l’ESMA e l’EIOPA saranno coinvolti nel promuovere discussioni al riguardo. Le autorità competenti potranno richiedere pareri alle Autorità Europee di Vigilanza in merito a particolari classificazioni o casi specifici richiesti da offerenti o soggetti richiedenti l’ammissione alla negoziazione. Tuttavia, la corretta classificazione delle cripto-attività resta principalmente responsabilità degli offerenti stessi, sebbene le autorità preposte possano contestarla sia prima che dopo la pubblicazione dell’offerta. Entrando nel dettaglio del regolamento MiCA, questo introduce una classificazione delle cripto-attività in tre macro-categorie principali, ciascuna soggetta a requisiti peculiari basati sui rischi associati. Gli

articoli 3 e 4 del Regolamento (UE) 2023/1114 definiscono questa suddivisione: “token di moneta elettronica”, “token collegati ad attività” e “altri token di cripto-attività”.

Chiarito il panorama normativo europeo e nazionale di riferimento è bene dedicare attenzione fatto secondo cui la blockchain potrebbe trovare applicazione alla contrattualistica del lavoro.

In questo rapporto si registra la presenza di soggetti come lavoratore, datore di lavoro, istituti previdenziali e assicurativi, ed organi ispettivi.

Tra tali attori che esercitano il loro ruolo nell’ambito del contratto di lavoro esistono vari obblighi di comunicazione: si pensi ad esempio all’obbligo che incombe sul datore di lavoro di inviare il modulo Unificato Lav, oppure alle incombenze da rispettare nei confronti centri per l’impiego, dell’Inps e dell’Inail.

Per quanto riguarda, invece, gli aspetti economici che caratterizzano il rapporto di lavoro si pensa al fatto che in alcuni casi le somme vengono versate ma non percepite da lavoratore: proprio al cospetto degli elementi che caratterizzano i rapporti di lavoro, a parere della dottrina, entra in gioco la tecnologia blockchain che rappresenterebbe la soluzione di molti problemi⁷¹.

In pratica basterebbe ricorrere, così come accade nella blockchain, all’istituzione di un registro unico decentrato al quale tutti gli operatori del rapporto potrebbero fare accesso promuovendo, ognuno limitatamente alla propria competenza, un blocco immodificabile della catena del rapporto che eviterebbe eventuali manomissioni ed azioni fraudolente a danno dei lavoratori: tale sistema realizzerebbe anche un altro vantaggio ossia quello di scongiurare illecite fattispecie di intermediazione o interposizione⁷².

La creazione di un modello simile di regolazione del rapporto di lavoro, con il supporto della tecnologia blockchain, sarebbe possibile solo nel momento in cui lo Stato riuscisse a superare il dogma di essere il solo accentratore materiale di tutte le funzioni regolative del rapporto per accettare, invece, il ruolo di semplice partecipante collocato sullo stesso piano degli altri soggetti che partecipano al rapporto di lavoro⁷³.

5. La tokenizzazione della ricchezza.

Strettamente connesso alla tecnologia blockchain è il concetto di “token”, termine inglese che significa *simbolo*, l’utilizzo di tale terminologia ha trovato ampio spazio in ambito informatico e rappresenta un processo in grado di proteggere un significato che non si vuole rendere noto.

⁷¹ V. LEMMA, *Quali controlli per le valute virtuali?* Op. cit., pag. 53 ss.

⁷² D. GAROFALO, *Blockchain, smart contract e machine learning: alla prova del diritto del lavoro*, in *Il lavoro nella giurisprudenza*, n. 10/2019, pag. 869 ss.

⁷³ D. GAROFALO, *op.cit.*, pag. 871 ss.

Dopo aver precisato cosa si intende con il termine token, con l'ausilio della dottrina si affronterà il tema della tokenizzazione della ricchezza.

Con questa espressione si intende la conversione della ricchezza in token digitali che vengono successivamente emessi su piattaforme a loro volta basate su una blockchain tramite uno *smart contract*.

La tokenizzazione della ricchezza permette quindi, tramite un meccanismo crittografico, la trasformazione di un dato sensibile in un dato non significativo e tale processo, a parere della dottrina comporta una serie di vantaggi⁷⁴.

Il primo di tali vantaggi coincide con una maggiore liquidità poiché permette di frammentare i titoli di proprietà di un bene e di crearne, quindi, un mercato secondario.

L'altro vantaggio coincide con l'aumento della velocità con la quale le transazioni possono essere effettuate ed una corrispondente diminuzione dei costi anche grazie all'automazione garantita dagli *smart contract*⁷⁵.

Tra gli altri risvolti positivi della tokenizzazione vi è anche una maggiore trasparenza garantita dall'immutabilità della blockchain, una riduzione dei costi della transazione che comporta fra l'altro come conseguenza un corrispondente aumento anche della platea dei soggetti investitori⁷⁶.

Almeno a prima vista questa nuova pratica è stata accolta come una novità che avrebbe avuto effetti sorprendenti nel mondo degli affari, ma l'entusiasmo iniziale non ha tenuto conto delle diverse questioni giuridiche direttamente connesse alla tokenizzazione: soprattutto per quanto concerne il diritto di proprietà e gli effetti della tokenizzazione sui titoli di credito.

Cominciamo ad esaminare, quindi, quali siano gli effetti della tokenizzazione sulla proprietà che comporta la possibilità di individuare nuove forme di titolarità sui beni che si discostano apertamente da quelle classiche.

Ma per comprendere a fondo come funziona tale meccanismo può essere utile analizzare un esempio. Supponiamo che un soggetto sia proprietario di un immobile ma sia a corto di liquidità: in questo caso potrebbe avere necessità di disporre di denaro per una somma inferiore rispetto al valore dell'immobile. Ove si verifichi tale eventualità, normalmente, si ricorre ad un prestito costituendo un'ipoteca sull'immobile.

⁷⁴ P. LAURENT, T. CHOLLET, M. BURKE, T. SEERS, *The tokenization of assets is disrupting the financial industry. Are you ready?*, in *Inside magazine*, issue 19, Part 02. Cfr. invece, in senso prettamente critico, E.-P. SCHUSTER, *Cloud Crypto Land*, LSE Law, *Society and Economy Working Papers*, 2019, 17.

⁷⁵ Per una definizione del concetto di *smart contract*, vedasi: D. GAROFALO, *Blockchain, smart contract e machine learning: alla prova del diritto del lavoro*, in *Il lavoro nella giurisprudenza*, n. 10, 2019, pag. 872, ove precisa che «Con l'espressione *smart contract* si intende, nella sua tradizione letterale, contratto intelligente. Si tratta di un contratto nel quale il sistema consente ad un venditore di vedersi accreditare la somma richiesta nello stesso identico momento nel quale l'acquirente manifesta la volontà di accettare le condizioni proposte per l'acquisto del bene...»

⁷⁶ R. DE CARIA, *Il diritto di fronte alla tokenizzazione dell'economia*, in *Il diritto dell'economia*, 1, 2020, pag. 857 ss.

Con la tokenizzazione della ricchezza si converte la proprietà tradizionale in una *smart property*, in questo modo il titolo di proprietà viene frazionato in una grande quantità di piccole unità (i *token*) e, queste unità, possono essere cedute a soggetti interessati all'investimento ricorrendo ad uno *smart contract* del quale resta traccia definitiva su una blockchain⁷⁷.

Il sistema che la tokenizzazione vorrebbe realizzare, quindi, attraverso la *smart property* consiste nella frammentazione del diritto di proprietà in un numero indefinito di rapporti suscettibili di essere trasferiti a terzi in un mercato secondario.

Un sistema simile, per quanto possa garantire liquidità maggiore e celerità nei trasferimenti, incontra non pochi ostacoli nel nostro ordinamento che necessita sempre dell'intermediazione notarile per garantire l'opponibilità a terzi del trasferimento immobiliare⁷⁸.

Tuttavia, è doveroso puntualizzare che, almeno a prima vista, nella tokenizzazione della ricchezza viene addirittura superata la necessità di ricorrere all'intermediazione notarile, dato che la certezza del trasferimento e l'opponibilità a terzi sarebbe comunque garantita con l'immutabilità della blockchain. Tale operazione, però, sarebbe impossibile soprattutto negli ordinamenti con notariato di tipo latino come il nostro.

A conferma della resistenza del nostro ordinamento rispetto all'avvento della *smart property* registra solo uno studio del Consiglio Nazionale del Notariato ma è bene puntualizzare che lo stesso si è limitato solo ad affrontare le problematiche applicative sollevate dall'intervento legislativo che ha introdotto nel nostro ordinamento il concetto di tecnologie basate su registri distribuiti e di *smart contract*⁷⁹.

Sul tema, inoltre, si registrano anche altri interventi⁸⁰ tutti protesi ad evidenziare la natura dirompente di tutte le innovazioni connesse alla blockchain non solo per la professione notarile, ma in senso più ampio anche per le categorie civilistiche tradizionali.

⁷⁷ Cfr. in argomento, *ex multis*, R. MORONE, *Smart properties*, in R. Battaglini, M. Tullio Giordano (a cura di), *Diritto della blockchain*, cit., 447-455; nella letteratura in inglese, v. già nel 2014, T. SWANSON, *Great Chain of Numbers: A Guide to Smart Contracts, Smart Property and Trustless Asset Management*, Capitolo 4 (Smart Contracts); v. poi A. WRIGHT, P. DE FILIPPI, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, in <https://ssrn.com/abstract=2580664> (2015), in particolare 33 ss.; v. anche, lo stesso anno, J.A.T. FAIRFIELD, *BitProperty*, in *S. Cal. L. Rev.*, 2015, 88, 805 ss.; v. infine L. GRIGGS, R. THOMAS, R. LOW, J. SCHEIBNER, *Blockchains, Trust and Land Administration – The Return of Historical Provenance*, in *Property Law Review*, 2017, 6, 180 ss.

⁷⁸ fr. in generale sul tema, tra i moltissimi, A. CIATTI CAIMI, *Della trascrizione degli atti relativi ai beni immobili [artt. 2643-2645-bis, 2646-2651]*, Milano, 2018; N.A. CIMMINO, *La trascrizione immobiliare*, Milano, 2012; F. GAZZONI, *La trascrizione immobiliare*, Milano, 3 volumi, 1991-1998; S. PUGLIATTI, *La trascrizione: l'organizzazione e l'attuazione della pubblicità patrimoniale*, Milano, 1989 (in *Trattato di diritto civile e commerciale* a cura di Cicu e Messineo); F.S. GENTILE, *Trascrizione (voce)*, in *Novissimo Digesto*, Torino, 1973, vol. XIX; L. FERRI, *Art. 2643-2696: Trascrizione immobiliare*, in *Commentario del Codice civile* a cura di Scialoja e Branca, Bologna - Il Foro Italiano, Roma, 1962; in epoca precedente all'attuale codice civile, v. anche N. COVIELLO, *Trascrizione (voce)*, in *Nuovo Digesto Italiano*, vol. XII, Torino, 1940; L. COSATTINI, *Trascrizione (voce)*, in *Enc. Italiana Treccani*, 1937, Roma; N. COVIELLO, *Della trascrizione*, 2 volumi, Torino, 1933.

⁷⁹ Art. 8-ter d.l. 135/2018.

⁸⁰ S. ACETO DI CAPRIGLIA, *Contrattazione algoritmica. Problemi di profilazione e prospettive operazionali. L'esperienza "pilota" statunitense*, in *federalismi.it*, 2019, 18, 2 ottobre 2019, segnatamente 55 ss.; M. KROGH,

Il ricorso alla tecnologia blockchain, come evidenziato dalla dottrina, potrebbe avere come effetto quello di “disintermediare” i trasferimenti di ricchezza, con la conseguenza che verrebbe addirittura superata la certezza tradizionalmente garantita dalla funzione notarile⁸¹.

Pur mantenendo un atteggiamento di fiduciosa apertura nei confronti dell'ondata innovativa prodotta dalle innovazioni tecnologiche che coinvolgono molte transazioni, i notai hanno evidenziato che l'avvento delle criptovalute⁸² ha generato innumerevoli dubbi in merito al fatto se ricondurre la categoria degli *smart contract* nella generica nozione codicistica di contratto⁸³.

In un primo momento l'idea di preservare il ruolo dei notai incorporando anche le blockchain all'interno delle loro attività è stato al centro di un progetto denominato NotharChain, iniziativa poi naufragata anche perché non teneva conto delle innumerevoli peculiarità che caratterizzano i vari tipi di blockchain.

Transazioni in monete virtuali e rischio di riciclaggio. Il ruolo del notaio, in *Notariato*, 2018, 2, 155 ss.; G. LAURINI, *Il notaio e le valute virtuali*, in *Notariato*, 2018, 2, 141 ss.; M. NASTRI, *Blockchain per i notai: opportunità e rischi*, in *www.agendadigitale.eu*, 30 maggio 2017; Federnotai Lombardia, *The blockchain system and its challenges*, in *Medialaws*, 23 febbraio 2017, poi ripreso nel manifesto *Smart contract and blockchain* reso pubblico dalla stessa Federnotai Lombardia e Università Bocconi in occasione del convegno *Blockchain: rivoluzione tecnologica e certezza del diritto* organizzato a Mila-no l'8 maggio 2017; M. MANENTE, *Blockchain e smart contract sono la risposta, ma a quale domanda?*, in *Biblioteca online della Fondazione Italiana del Notariato*, Atti del convegno “Atto notarile informatico: cosa cambia?” tenutosi a Torino il 16 giugno 2017.

⁸¹ C. LICINI, *Riusciranno i notai a non essere disintermediati nel mondo telematico?*, Parte I e Parte II, in *MediaLaws*, 11 febbraio 2019; v. anche R. MORONE, *Smart properties*, cit., specialmente 452 ss. (l'Autore è il Notaio che ha rogato la prima compravendita italiana di immobili con pagamento in Bitcoin: cfr. R. BOSIO, *Il primo atto immobiliare in “bitcoin” porta il sigillo del notaio Remo Morone*, in *enordovest*, 24 gennaio 2018).

⁸² Cfr. tra i molti P.R. AMENDOLA, B. MASCAGNI, *L'inquadramento delle criptovalute: TAR del Lazio, sent. n. 01077/2020 del 27 gennaio 2020*, in *Diritto Bancario*, 5 marzo 2020; V. DE STASIO, *Le monete virtuali: natura giuridica e disciplina dei prestatori di servizi connessi*, in M. CIAN, C. SANDEI (a cura di), *Diritto del Fintech*, Milano, 2020, 215 ss., specialmente 233 ss.; G. BERTOLINI, *Guida alle criptovalute. Inquadramento giuridico e cryptofunding*, in *Opinio Juris*, 6 luglio 2019; A. CALONI, *Bitcoin: profili civilistici e tutela dell'investitore*, in *Riv. Dir. Civ.*, 2019, 65(1), 159 ss.; A.M. GAMBINO, C. BOMPRESZI, *Blockchain e criptovalute*, in G. FINOCCHIARO, V. FALCE (a cura di), in *Fintech: diritti, concorrenza, regole*, Bologna, 2019, 267 ss.; C. LANFRANCHI, *Profili giuridici delle valute virtuali*, in *Cyberspazio e Diritto*, 2019, 1-2, 43; P. IEMMA, N. CUPPINI, *La qualificazione giuridica delle criptovalute: affermazioni sicure e caute diffidenze*, in *Diritto Bancario*, 8 marzo 2018; M. BELLEZZA, *Blockchain*, in M.-T. PARACAMPO (a cura di), *FinTech: Introduzione ai profili giuridici di un mercato unico tecnologico*, Torino, 2017, 217 ss.; R. BOCCHINI, *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in *Il Diritto dell'informazione e dell'informatica*, 2017, 1, 27 ss.; N. BUSTO, *Bitcoin tra “disintermediazione” e “iper-intermediazione”*, in *Cyberspazio e Diritto*, 2016, 3, 309 ss.; N. VARDI, *Bit by Bit: Assessing the Legal Nature of Virtual Currencies*, in G. GIMIGLIANO, *Bitcoin and Mobile Payments. Constructing a European Union Framework*, London, 2016, 55 ss.; G. BONAIUTI, *Le nuove forme di pagamento: una sintesi degli aspetti economici*, in *Analisi Giuridica dell'Economia*, 2015, 1, 17 ss.; N. VARDI, *“Criptovalute” e dintorni: alcune considerazioni sulla natura giuridica del “Bitcoin”*, in *Il Diritto dell'informazione e dell'informatica*, 2015, 15 (3), 443 ss.

⁸³ R. DE CARIA, *The Definition(s) of Smart Contracts Between Law and Code*, in M. CANNARSA, L.A. DIMATTEO, C. PONCIBÒ (a cura di), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, Cambridge, 2019, 19 ss.

6. Blockchain e problematiche giuridiche: coordinamento con la normativa in materia di documenti informatici, validazione temporale e protezione dei dati personali.

Dalle tematiche analizzate finora si evince come, nel corso del tempo, la tecnologia influisca in modo decisivo sul modo in cui i consociati regolano le proprie relazioni pertanto non può ignorarsi che essa condizioni il diritto che governa la società⁸⁴.

Anche l'avvento della tecnologia blockchain sta determinando un mutamento delle relazioni umane, e la creazione di un mondo virtuale dove ormai si compongono molte relazioni, e nel quale è possibile accedere con la creazione di una identità digitale che rappresenta il ponte fra mondo reale e mondo virtuale, può essere fonte di problemi soprattutto attinenti al trattamento dei dati personali ed ai pericoli che dalla loro gestione inadeguata possono scaturire⁸⁵.

È evidente che al cospetto dell'ampio utilizzo dei servizi offerti della rete, luogo dove ormai nascono innumerevoli transazioni, diventa fondamentale proteggere tutte le proiezioni della persona umana all'interno del mondo virtuale⁸⁶.

Ma prima di soffermarsi sulle problematiche che scaturiscono in materia di protezione dei dati personali ed utilizzo della tecnologia blockchain è bene ricordare, nuovamente, le caratteristiche di quest'ultima⁸⁷.

La blockchain può essere assimilata, in modo piuttosto semplicistico, ad un registro o a un libro mastro digitale che conserva in modo immutabile le transazioni avvenute ove, ciascun partecipante, ha a sua disposizione una copia di ogni operazione.

La blockchain, quindi, è una specie del genere DLT (Distributed ledger technologies) tecnologia basate su registri distribuiti.

Le caratteristiche principale che contraddistinguono la blockchain, sono come già anticipato, le seguenti: la disintermediazione, la decentralizzazione, immutabilità inalterabilità e persistenza dei dati⁸⁸, nonché la validazione temporale e crittografica asimmetrica⁸⁹.

⁸⁴ G. PASCUZZI, *Il diritto dell'era digitale*, Bologna, 2002, 61-66, dove l'Autore pone in evidenza il fatto che la tecnologia da un lato determina il verificarsi di nuove situazioni che possono minare la riservatezza degli individui, dall'altro predispone anche dei rimedi da utilizzare per la difesa dei propri dati personali.

⁸⁵ M. GIULIANO, *La blockchain e gli smart contracts nell'innovazione del diritto del terzo millennio*, in *Diritto dell'informazione e dell'informatica*, fasc. 6, 1° dicembre 2018, pag. 989 ss.

⁸⁶ Internet nasce come ARPANet (dal nome dell'agenzia di ricerca americana che l'aveva progettata, Advanced Research Project Agency) nel 1969 con l'obiettivo di realizzare un flessibile strumento di comunicazione adatto a garantire il collegamento tra strutture militari, anche in caso di interruzioni delle linee principali di comunicazione (V. A. APARO, *Il libro delle reti*, Roma, 1995). V. LEMMA, *Quali controlli per le valute virtuali?* in *Riv. Trim. di diritto dell'economia*, suppl. n. 3 al n.1/2022, pag. 53 ss.

⁸⁷ F. FAINI, *Blockchain e diritto: la catena del valore tra documenti informatici, smart contracts e data protection*, in *Responsabilità civile e Previdenza*, fasc. 1, 1° gennaio 2020, pag. 299 ss.

⁸⁸ Al riguardo, è opportuno precisare che l'immodificabilità non è una caratteristica valida in assoluto: l'immodificabilità va intesa da un punto di vista unilaterale (un singolo da solo non può modificare i dati), ma laddove si pervenisse a un controllo sulla maggioranza del consenso diventerebbe possibile. F. FAINI, *op.cit.*, nota n. 12.

⁸⁹ Si tratta di un sistema a doppia chiave pubblica e privata: la chiave privata è conosciuta e utilizzata dal soggetto titolare per cifrare i dati; la chiave pubblica è l'elemento utilizzato dal destinatario per decifrare i dati e verificare l'utente (ciò non consente la diretta riferibilità all'identità del soggetto, in particolare nelle *permissionless*).

La disciplina della tecnologia blockchain si divide fra normativa europea e nazionale, precisando che la prima ha fortemente sostenuto, anche tramite la creazione dell'European Blockchain Service Infrastructure (EBSI), che l'utilizzo di tale nuova tecnologia sia assistita da elevati standard di sicurezza e protezione dei dati personali⁹⁰.

A livello nazionale l'articolo 8 ter del decreto-legge 135/2018, convertito in legge 12 del 2019 ha definito le tecnologie basate su registri distribuiti (DLT) sovrapponendola alla blockchain che invece ricordiamo è solo una specie del più ampio genere DLT con peculiarità autonome e distintive⁹¹.

La norma in questione chiarisce che la memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporanea elettronica previsti dall'articolo 41 del Regolamento Ue 910/2014, precisando che tale disposizione prevede tanto la validazione temporale semplice quanto la validazione temporale qualificata: queste due distinte tipologie di validazione temporale, però, differiscono da un punto di vista giuridico⁹².

Infatti, per poter aver una presunzione di certezza della data, e dell'ora nonché dell'integrità dei dati bisogna fare ricorso alla validazione temporale qualificata⁹³, mentre in caso di validazione semplice la valutazione dell'attendibilità di tali dati e della loro collocazione temporale è rimessa all'apprezzamento del giudice⁹⁴.

Considerato il differente valore probatorio che attribuiscono al documento informatico le validazioni temporali semplici e qualificate, non si comprende per quale ragione il legislatore nazionale rinvia all'articolo 41 del Regolamento UE e IDAS 910/2014, senza chiarire a quale delle due validazioni si riferisce⁹⁵.

Le due chiavi sono correlate e indipendenti. La crittografia asimmetrica caratterizza anche la firma digitale, con la differenza che nel caso della blockchain non ci sono certificati qualificati e prestatori di servizi fiduciari qualificati, presenti invece nel meccanismo della firma digitale. F. FAINI, *op.cit.*, nota n. 14.

⁹⁰ L'European Blockchain Services Infrastructure (EBSI) prenderà forma come una rete di nodi distribuiti in tutta Europa e diventerà un Building Block del Connecting Europe Facility (CEF), fornendo software, specifiche e servizi riutilizzabili per supportarne l'adozione da parte delle istituzioni dell'Unione Europea e delle Pubbliche Amministrazioni europee.

⁹¹ Sull'analisi della norma cfr. C. BOMPRESZI, *Commento in materia di Blockchain e Smart contract alla luce del nuovo Decreto Semplificazioni*, in *Dir. merc. tecn.*, 2019, pag. 6 ove riassume i profili critici dell'art. 8-ter del d.l. n. 135/2018, convertito in legge n. 12/2019, nell'imprecisione delle definizioni, nella superfluità di alcune disposizioni e nel rischio di limitare l'evoluzione tecnologica (e non incentivarla in coerenza alle intenzioni); F. SARZANA DI SANT'IPPOLITO, *Blockchain e smart contract nel nuovo decreto semplificazioni*, in *Dir. Internet*, 2019, 17-23; F. FAINI, *op.cit.*, nota n. 23.

⁹² Art. 8-ter, commi 3 e 4, d.l. n. 135/2018, convertito in legge n. 12/2019.

⁹³ Art. 41, par. 2, Reg. (UE) eIDAS n. 910/2014. La validazione temporale elettronica qualificata è definita dall'art. 3, par. 1, n. 34, e i requisiti che deve soddisfare sono stabiliti nell'art. 42, Reg. (UE) eIDAS n. 910/2014.

⁹⁴ La validazione temporale elettronica semplice è definita dall'art. 3, par. 1, n. 33), Reg. (UE) eIDAS n. 910/2014.

⁹⁵ Cfr. C. BOMPRESZI, *op. cit.*, 5 ss.

Considerando che è cosa ben diversa la validazione temporale qualificata rispetto a quella semplice bisogna capire come comportarsi a fronte dei dubbi creati dalla normativa in questione.

Un ausilio a tal riguardo per sciogliere questo nodo interpretativo potrebbe derivare dagli standard tecnici individuati dall'AGID (Agenzia per l'Italia digitale) che devono soddisfare le tecnologie basate sui registri distribuiti.

Tuttavia, neanche tali standard tecnici fissati dall'Agid riescono a fornire una risposta chiara in merito alla valenza delle due distinte tipologie di validazione temporale⁹⁶.

Per oltrepassare l'incertezza che domina l'argomento bisogna oltrepassare i confini della disciplina nazionale per soffermarsi, ancora una volta, sul Regolamento UE eIDAS n. 910/2014 che fissa un principio di non discriminazione fra le due distinte tipologie di validazione stabilendo al primo paragrafo dell'articolo 41 quanto segue: «alla validazione temporanea elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziari per il solo motivo nella sua forma elettronica o perché non soddisfa i requisiti della validazione temporanea elettronica qualificata».

Tenendo conto di tale principio quindi l'unico modo per oltrepassare i dubbi generati dall'incertezza letterale della norma, è possibile solo ipotizzando che il legislatore intendesse fare riferimento alla validazione temporale elettronica qualificata anche perché, se fosse stato il contrario, avrebbe palesemente limitato quanto previsto a livello europeo dal principio di non discriminazione appena menzionato.

Inoltre, è doveroso precisare ulteriormente, che propendere per la validazione temporale qualificata tenendo conto degli standard qualitativi previsti dall'Agid sarebbe stata una scelta inadeguata: considerando che le disposizioni ivi contenute debbano considerarsi solo alla stregua di strumento di supporto finalizzate a garantire il rispetto dei requisiti previsti dal Regolamento Europeo 910/2014 non potendo, i principi dell'Agid, sostituirsi alla disciplina contenuta in un regolamento europeo che, ricordiamolo, prevale sulle norme nazionali che si pongano in contrasto con lo stesso⁹⁷.

A titolo di completezza è bene precisare che in tema di validazione temporale elettronica qualificata rilevano anche il considerando n. 62 del Regolamento UE Eidas secondo il quale «al fine di garantire la sicurezza della validazione temporale elettronica qualificata, il ... regolamento dovrebbe richiedere l'uso di un sigillo elettronico avanzato o di una firma elettronica avanzata o di altri metodi equivalenti»; lo stesso considerando inoltre ritiene «prevedibile che l'innovazione produca nuove tecnologie in grado di assicurare alla validazione temporale un livello di sicurezza equivalente. Ogni qualvolta venga utilizzato un metodo diverso dal sigillo elettronico avanzato o dalla firma elettronica avanzata, dovrebbe spettare al prestatore di servizi fiduciari qualificato

⁹⁶ V. LEMMA, *Quali controlli per le valute virtuali?*, op. cit., pag. 53 ss.

⁹⁷ C. BOMPRESZI, *op. cit.*, pag. 6.

dimostrare, nella relazione di conformità, che tale metodo garantisce un livello equivalente di sicurezza e soddisfa gli obblighi previsti».

Dopo aver chiarito la valenza della validazione temporale qualificata, che rappresenta la forma adeguata per fornire la prova del dato e del giorno e dell'ora in cui lo stesso è stato inserito nella blockchain, è necessario dedicare cenno ad una delle questioni che implica l'utilizzo di tale nuova tecnologia rispettando i principi fissati dal Regolamento europeo 2016/679 in materia di protezione dei dati personali⁹⁸.

A tal proposito è evidente che nella tecnologia blockchain, al contrario di quello che accade in una tradizionale applicazione web in cui dati sono conservati in un server, i dati sono distribuiti su un network, e la trasparenza che caratterizza tale tecnologia, permette che gli stessi siano accessibili ad un numero vastissimo di individui. Pertanto, se la trasparenza rappresenta, senza alcun dubbio, uno delle caratteristiche più apprezzabili della tecnologia blockchain, d'altra parte può anche rappresentare una minaccia che scaturisce proprio dalla conoscenza illimitata degli stessi dati contenuti nella blockchain⁹⁹.

In particolare, nella tecnologia blockchain la replica dei dati nelle varie copie scaricate nei server dei nodi estranei per le finalità per cui gli stessi sono stati condivisi è evidente che entra in conflitto con il principio di minimizzazione del trattamento dei dati per il quale si richiede che siano “adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati”.

È evidente che l'utilizzo dei dati immessi nella blockchain da ciascun partecipante per finalità diverse rispetto alle quali gli stessi sono stati trattati, collide chiaramente con i principi previsti dal Regolamento europeo in materia di protezione dei dati¹⁰⁰, compromettendo concretamente il diritto dei partecipanti ad ottenere protezione effettiva dei dati¹⁰¹.

⁹⁸ A.M. GAMBINO, C. BOMPRESZI, *Blockchain e protezione dei dati personali*, in *Diritto dell'Informazione e dell'Informatica*, fasc. 3, 1 giugno 2019, pag. 628 ss.

⁹⁹ M. BERBERICH, M. STEINER, *Blockchain technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers?*, op. cit., 425

¹⁰⁰ *Ex art. 1 Reg.*, oggetto dello stesso è la protezione dei “dati personali”, i quali vengono definiti ex art. 4, par. 1, n. 1, come «qualsiasi informazione riguardante una persona fisica identificata o identificabile». Se la persona fisica non è identificata, né identificabile, il dato non è personale, ma anonimo. Pertanto, i dati anonimi non vengono tutelati dal GDPR, come anche esplicitato dal cons. n. 26 («I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazione che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche e di ricerca»). A.M. GAMBINO, C. BOMPRESZI, op.cit, pag. 628, nota 72.

¹⁰¹ Il Parlamento Europeo, nella Risoluzione del 3 ottobre 2018 sulle “tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione (2017/2772(RSP))” sottolinea che è della massima importanza che gli usi del DLT siano conformi alla legislazione dell'UE sulla protezione dei dati, in particolare al regolamento generale sulla protezione dei dati (GDPR) ed invita la Commissione e il Garante europeo della protezione dei dati (GEPD) a fornire ulteriori orientamenti su questo punto. Il Parlamento inoltre evidenzia che la DLT promuove la pseudonimizzazione degli utenti, ma non la loro anonimizzazione. Cosicché, se la pseudonimizzazione impedisce l'identificazione del soggetto senza l'utilizzo di informazioni aggiuntive, tuttavia non è una tecnica che

Proprio le caratteristiche della blockchain prima richiamate (trasparenza, irreversibilità, disintermediazione, etc.), devono necessariamente conciliarsi con i principi fissati dal GDPR (Regolamento europeo generale sulla Protezione dei Dati)¹⁰².

Uno dei primi problemi che genera la strutturazione della blockchain, fondata su un modello di consenso unanime o maggioritario di accesso ai dati, è insito nella difficoltà di risalire al responsabile del trattamento dei dati personali¹⁰³. Ovviamente chiarire tale aspetto riveste un'importanza fondamentale nel momento in cui si assiste ad un illecito trattamento dei dati personali.

Per risalire al soggetto responsabile del trattamento dei dati personali si procede in modo distinto a seconda dei casi.

Infatti, nel caso di registri centralizzati responsabile del trattamento dei dati personali sarà l'autorità centrale che gestisce e valida le informazioni contenute nei registri. La situazione cambia nel caso di registri distribuiti sui quali opera la blockchain, ove a fronte della delocalizzazione e polverizzazione dei nodi che la compongono, allo stato attuale non è possibile risalire al responsabile del trattamento dei dati.

Si potrebbe risolvere tale problematica garantendo, anche per i dati che confluiscono nelle blockchain, il rispetto della GDPR, ed in assenza di una normativa certa è indispensabile ricorrere ad un'interpretazione estensiva delle principali disposizioni previste dal GDPR soprattutto riguardo quelle che riconoscono i seguenti diritti agli interessati: a) il diritto di rettifica, b) il diritto all'oblio o di cancellazione; c) il diritto alla limitazione del trattamento; d) il diritto alla portabilità del dato.

Questo sforzo interpretativo è indispensabile per garantire una tutela effettiva dei dati personali fino a quando non si assisterà all'intervento del legislatore che riesca a colmare le lacune in materia.

Solo ricorrendo all'interpretazione estensiva dei principi previsti dal GDPR si eviterà che gli operatori che operano nel mercato blockchain siano costretti a dotarsi di sistemi in grado di assicurare il massimo livello di garanzie previste proprio da tale regolamento.

impedisce in assoluto l'impossibilità di identificare la persona che si celi dietro il dato. Vedasi sul tema il contributo di: M. GIULIANO, *Blockchain e gli smart contracts nell'innovazione del diritto del terzo millennio*, in *Diritto dell'Informazione e dell'innovazione tecnologica*, fasc. 6, 1 dicembre 2018, pag. 989 nota n. 64.

¹⁰² Si veda CNIL, September 2018 “*Blockchain et RGPD: quelles solutions pour un usage responsable en présence de données personnelles?*”.

¹⁰³ Ai sensi dell'art. 26.3 GDPR: “*l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento*”. Se tutti i nodi partecipanti alla blockchain (di numero indefinito) fossero qualificati come titolari del trattamento di tutti i dati processati sulla blockchain, si determinerebbe un ostacolo decisivo all'operatività di tale tecnologia.

Il primo raffronto che bisogna fare, per stabilire il rispetto da parte della blockchain, dei principi del GDPR riguarda proprio il diritto di rettifica previsto dall'articolo 16 che riconosce all'interessato il diritto di richiedere al titolare del trattamento dei dati la rettifica degli stessi.

Il rispetto di tale diritto non sembra conciliarsi con l'immutabilità dei dati che, come più volte ribadito, caratterizza le blockchain. A tal riguardo la dottrina evidenzia che l'unico rimedio possibile sarebbe quello di consentire all'interessato una rettifica¹⁰⁴. Nel caso di blockchain tale rettifiche dovrebbe essere possibili solo attraverso l'inserimento di un ulteriore blocco di dati volto a rettificare il blocco precedente¹⁰⁵.

Per quanto riguarda il diritto di accesso previsto dall'art. 15 del GDPR, l'interessato ha il diritto di ottenere dal responsabile del trattamento dei dati personali informazioni riguardanti l'eventuale trattamento di dati personali a lui riferiti, ed al contempo l'interessato può ottenere anche una serie di informazioni aggiuntive riguardanti le finalità del trattamento, nonché i destinatari ai quali i dati verranno comunicati.

In base alle disposizioni contenute dal GDPR, se i dati dell'interessato vengono trasferiti ad un paese terzo l'interessato ha il diritto di esserne informato in merito al fatto se sussistono garanzie adeguate. Proprio tale informativa sarebbe particolarmente adeguata in caso di trasferimento di dati tramite blockchain, dato che la stessa garantisce la condivisione dei dati fra tutti i nodi dei partecipanti a prescindere dalla loro collocazione geografica.

Tuttavia, anche tale possibilità deve essere esclusa poiché i nodi validanti delle transazioni blockchain non sono a conoscenza dei dati criptati dei singoli blocchi, ragion per cui l'accesso garantito previsto dal GDPR risulta assolutamente incompatibile con la blockchain¹⁰⁶.

Un ultimo cenno deve essere dedicato, infine, al diritto alla cancellazione dei dati (c.d. diritto all'oblio) nella blockchain, ma procediamo per gradi affermando in primo luogo che l'articolo 17 del GDPR disciplina il diritto dell'interessato alla cancellazione al ricorrere delle condizioni elencate dal primo comma della norma¹⁰⁷.

¹⁰⁴ A. RICCI, *Il Nuovo Regolamento Europeo sulla Protezione dei Dati Personali*, Bologna, 2018, p.193. L'autrice rileva in particolare come ad oggi le richieste di rettifica nell'esperienza applicativa del Garante per la protezione di dati personali si siano limitate sostanzialmente all'aggiornamento dei registri dei battezzati.

¹⁰⁵ V. FERRARI, *EU Blockchain Observatory and Forum Workshop on GDPR, Data Policy and Compliance*, University of Amsterdam, p. 8.

¹⁰⁶ M. FINCK, *Blockchains and Data Protection in EU*, Max Plank institute for Innovation and Competition Research, paper n. 18-01, p. 23.

¹⁰⁷ Il primo comma dell'articolo 17 del GDPR dispone: «L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti: a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento; c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2; d) i dati personali sono stati trattati illecitamente; e) i dati personali devono essere cancellati per adempiere un obbligo giuridico

Anche in quest'ultimo caso considerate le caratteristiche che contraddistinguono la blockchain, prima fra tutte l'immutabilità dei dati, si ritiene che il principio della cancellazione dei dati sensibili non possa trovare applicazione nella blockchain.

Alcuni autori, nel tentativo di estendere l'applicabilità di tale principio anche alla blockchain, hanno suggerito che una soluzione possibile poteva essere quella di implementare le procedure formali per la cancellazione delle chiavi di accesso ai dati della catena. In tal modo i dati continuerebbero ad esistere sulla catena blockchain ma nessuno avrebbe la possibilità di accedervi¹⁰⁸.

A conferma dell'impossibilità di estendere il principio del diritto alla cancellazione dei dati anche nell'utilizzo della tecnologia digitale, basta pensare che gli stati membri hanno dimostrato una chiara resistenza anche perché il GDPR non definendo il concetto di cancellazione consente ampi margini di discrezionalità.

Per fare un esempio a tal riguardo si pensi al fatto che uno Stato come la Germania che nell'ambito della legge nazionale sulla protezione dei dati stabilisce che il dato non possa essere distrutto se specifici mezzi di archiviazione rendono impossibile tale operazione, ed in tal modo si accetta come unica alternativa solo quella della limitazione del trattamento nulla disponendo sulla cancellazione vera e propria¹⁰⁹.

In un contesto caratterizzato da una notevole complessità tecnica, unita ad una velocità di sviluppo che va di pari passo con quella della tecnologia digitale, si pone la necessità di porre in essere una costante opera di aggiornamento e studio del fenomeno che, di sicuro, vede avanti a sé un'ulteriore e continua espansione. L'ingresso in questo mercato da parte dei giganti dell'industria IT (ne è un esempio il progetto di "Libra", la criptovaluta di Facebook), oltre ad una crescente attenzione al fenomeno non fa altro che stimolare la volontà di connessioni di questi fenomeni con l'economia reale; motivo per cui va tenuta alta l'attenzione da parte di tutti gli attori istituzionali.

previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1».

¹⁰⁸ P. DE FILIPPI, *The Interplay between Decentralization and Blockchains: The Case of Blockchain Technologies*, 2016, 9 *Journal of Peer Production*, p. 1.

¹⁰⁹ Come contributo sul tema si segnala il contributo di G. M. RICCIO, G. SCORZA E E. BELISARIO, *GDPR e normativa Privacy*, commentario, Padova, 2017, p. 179.