LUISS

Dipartimento
di Scienze Politiche

Cattedra : Diritto dell'Unione Europea

La regolamentazione della tecnologia blockchain nell'Unione Europea: dal GDPR agli Smart Contract

Prof. Francesco Cherubini
RELATORE

Daniele Marconi Matr. 085042
CANDIDATO

Anno Accademico 2019/2020

INDICE

INTRODUZIONE

"We know there will be challenges as Distributed Ledgers mature and disrupt how we think about and store data"[1].

Sono passati ormai undici anni, da quando la prima e allora più fortunata applicazione della tecnologia blockchain fu presentata al mondo da Satoshi Nakamoto (la cui identità rimane ancora celata) e la prima criptovaluta basata su blockchain fu generata: il bitcoin[2]. Da quel giorno, moltissimi nuovi ambiti di applicazione sono stati sperimentati, dalla tracciabilità e gestione della *supply chain* alla notarizzazione e certificazione, dalla finanza alla sanità, dal privato al pubblico. La tecnologia attualmente si trova in una nuova fase, forse la più delicata: quella della regolamentazione. Moltissime soluzioni e idee per implementazioni sono frenate dall'incertezza normativa. Alcuni Stati membri hanno voluto anticipare le normative europee nella definizione della tecnologia, come Malta, Estonia, Italia ecc.

Nel 2017, la Commissione stava "monitorando attivamente"[3] gli sviluppi delle iniziative blockchain. Il cosiddetto approccio *wait and see* ha sicuramente il merito di far progredire e ampliare gli ambiti di applicazione della blockchain, però, d'altra parte, la mancanza di regolamentazione specifica può portare ad abusi. Ovviamente, il contesto normativo attualmente esistente si applica alla blockchain, come avvenuto nel celebre caso riguardante il sito "Silk Road", un mercato nero online che si affidava ai pagamenti bitcoin, chiuso nel 2013[4]. La soft law, come ad esempio fornire dei principi guida, è un altro metodo per dirigere il cambiamento senza intervenire con la tradizionale regolamentazione vincolante; un caso lampante è stata la risoluzione del Parlamento Europeo del 2018 *building trust with disintermediation*[5], nella quale si enumerano le possibili applicazioni delle DLT e si tracciano linee guida d'azione per rendere l'Europa un player globale in tale ambito. Più recentemente, gli Stati membri e le istituzioni europee hanno inaugurato un periodo di cooperazione regolatoria, per coordinare gli sforzi ed evitare disomogeneità nel mercato interno, attraverso diverse iniziative.

Nel febbraio del 2018, la Commissione Europea ha avviato lo EU Blockchain Observatory and Forum il cui scopo è di "accelerate blockchain innovation

[1] Un report dello UK Government Chief Scientific Adviser del dicembre 2015 (pubblicato nel gennaio 2016), *Distributed Ledger Technology: beyond block chain*.
[2] NAKAMOTO (2009).
[3] PARKER (2017).
[4] PAGLIERY (2013).
[5] Risoluzione del Parlamento Europeo del 3 Ottobre 2018, P8_TA-PROV (2018)0373, *Distributed ledger technologies and blockchains: building trust with disintermediation*.

and the development of the blockchain ecosystem within the EU"[6]. Si occupa di delineare l'ecosistema in ambito blockchain all'interno dell'Unione Europea, mettere in comune esperienze e competenze, identificare le barriere che non permettono la piena realizzazione della tecnologia, proporre tavole rotonde europee[7].

Nell'aprile del 2018, 21 Stati membri (non l'Italia, che si è aggiunta successivamente) e la Norvegia hanno firmato una Dichiarazione che costituiva la European Blockchain Partnership ("EBI") e hanno cooperato per la realizzazione della European Blockchain Services Infrastructure ("EBSI") "that will support the delivery of cross-border digital public services"[8]. Ad oggi, il numero di Stati europei che partecipano è salito a trenta. Per promuovere la standardizzazione, la Commissione ha anche incoraggiato la nascita dell'International Association for Trusted Blockchain Applications ("INABTA") in Belgio, un forum che vanta tutti gli sviluppatori e gli utenti delle tecnologie blockchain a livello mondiale. Inoltre, la Commissione partecipa attivamente nel processo di standardizzazione a livello internazionale, per assicurarsi che sia in linea con i valori europei, nei consessi del Comitato europeo di normazione e Comitato europeo di normazione elettrotecnica (CEN/CENELEC), dell'Organizzazione internazionale per la normazione (ISO Technical Committee 307) o dell'Unione internazionale delle telecomunicazioni (ITU-T Focus Group su DLT).

Dal punto di vista economico, la Commissione ha previsto l'erogazione di numerosi fondi per progetti in ambito blockchain, soprattutto tramite il programma Horizon 2020. Un esempio è il premio "blockchain for social good", che consiste nello sviluppare soluzioni innovative in campo sociale basate su registri distribuiti.

[6] Come descritto dalla Commissione Europea sul sito ufficiale dello European Union Blockchain Observatory and Forum.
[7] ANONIMO (2019).
[8] Secondo la definizione elaborata dalla squadra responsabile "Digital Innovation and Blockchain (Unità F.3)" sul sito ufficiale della European Blockchain Services Infrastructure ("EBSI").

CAPITOLO 1. INQUADRAMENTO DELLA TECNOLOGIA BLOCKCHAIN

1.1 Definire la blockchain

Prima di addentrarsi in definizioni legali e nelle conseguenti implicazioni, è necessario soffermarsi sul funzionamento della tecnologia. La conoscenza del protocollo è propedeutica alla comprensione delle relazioni che si vengono a formare fra gli attori dell'ecosistema, la governance, la "cripto-economia"[9], i limiti normativi, e non solo, della tecnologia allo stato attuale.

Esistono numerose definizioni di blockchain, che si concentrano su diverse caratteristiche della stessa. Innanzitutto, è essenziale definire il rapporto tra blockchain e "Distributed Ledger Technologies" ("DLT"): le prime sono parte della più grande categoria delle seconde. Può essere utile quindi partire da una definizione delle DLT, termine introdotto nel 2015 dal report UK *Distributed Ledger Technology: beyond block chain*[10].

> Distributed ledgers are a type of database that is spread across multiple sites, countries or institutions, and is typically public. Records are stored one after the other in a continuous ledger, rather than sorted into blocks, but they can only be added when the participants reach a quorum[11].

Lo scopo principale dei registri distribuiti è, quindi, la registrazione di informazioni (e.g. transazioni) all'interno del "libro mastro" digitale.

Ogni transazione deve essere sottoposta ad una procedura di firma a doppia chiave asimmetrica, simile a quello della firma digitale. L'utilizzo di algoritmi crittografici, tramite una chiave pubblica e una chiave privata, permette all'utente di partecipare al network[12].

Le informazioni sono distribuite nei nodi[13] della rete, il risultato è un'architettura distribuita. Per distruggere il network sarebbe necessario eliminare tutti i nodi (in realtà basterebbe che il 50%+1 dei nodi avesse intenzioni malevole per compromettere la rete, il c.d. "51% attack"). Non esiste un "singolo punto di fallimento" perché non esiste un'autorità centrale.

---

[9] "La cripto-economia studia la progettazione di un sistema che opera in un ambiente avverso in cui imbrogliare (o tentare di imbrogliare) è meno conveniente rispetto a comportarsi onestamente, ovvero dove i benefici di un comportamento disonesto sono inferiori ai costi. Ciò si ottiene combinando crittografia e incentivi economici", secondo il contributo di CHIAP, RANALLI, BIANCHI (2019: 77).

[10] Un report dello UK Government Chief Scientific Adviser del dicembre 2015 (pubblicato nel gennaio 2016), *Distributed Ledger Technology: beyond block chain*.

[11] Ibid.

[12] BELLINI (2020).

[13] I nodi sono i partecipanti alla blockchain, le macchine connesse al network.

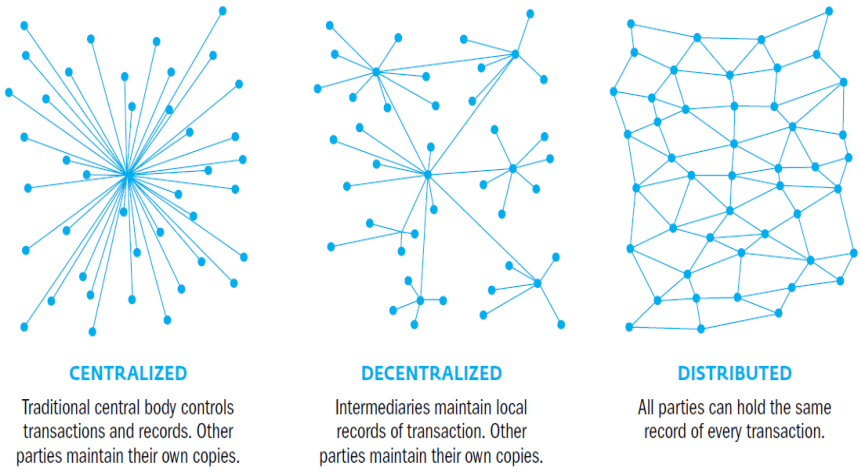


Figura 2. Evoluzione dei registri di Paul Baran, On distributed communications networks, 1964, and Marina Niforos, 2017[14].

La fiducia non è più in un'organizzazione intermediaria (e.g. una banca) ma nel sistema stesso.

Il registro può essere letto, verificato (trasparente) e alterato da tutti i nodi della rete (nel caso di blockchain "pubblica") ma a differenza di un database tradizionale, è possibile solamente aggiungere informazioni, non modificarle né tantomeno cancellarle (anche se in seguito vedremo che non è impossibile farlo). L'immutabilità è resa possibile dal meccanismo di validazione dei dati registrati sul *ledger,* il c.d. consenso, e dalla struttura del registro. Queste due caratteristiche sono ciò che permette di distinguere fra i diversi tipi di *Distributed Ledgers*.

> Block chain is a type of database that takes a number of records and puts them in a block (rather like collating them on to a single sheet of paper). Each block is then 'chained' to the next block, using a cryptographic signature. This allows block chains to be used like a ledger, which can be shared and corroborated by anyone with the appropriate permissions[15].

Le architetture blockchain sono quindi quelle dove il registro è strutturato in una catena di blocchi, contenenti più transazioni, tra di loro concatenati tramite crittografia (e.g. Bitcoin ed Ethereum)[16].

[14] Un report della International Finance Corporation (WB) del gennaio 2019 (prima stampa ottobre 2017), *Blockchain Opportunities for Private Enterprises in Emerging Markets*.
[15] Un report dello UK Government Chief Scientific Adviser del dicembre 2015 (pubblicato nel gennaio 2016), *Distributed Ledger Technology: beyond block chain*.
[16] VELLA (2019).

Ciascun blocco è un archivio di tutte le transazioni storiche validate, correlate da un marcatore temporale (*timestamp*). Inoltre, ogni blocco contiene l'*hash*[17] del blocco precedente. Così, in caso di manipolazioni, la modifica risulterebbe subito evidente. Infatti, cambiando il contenuto di un blocco, l'*hash* del medesimo sarebbe modificato e di conseguenza tutti i successivi.

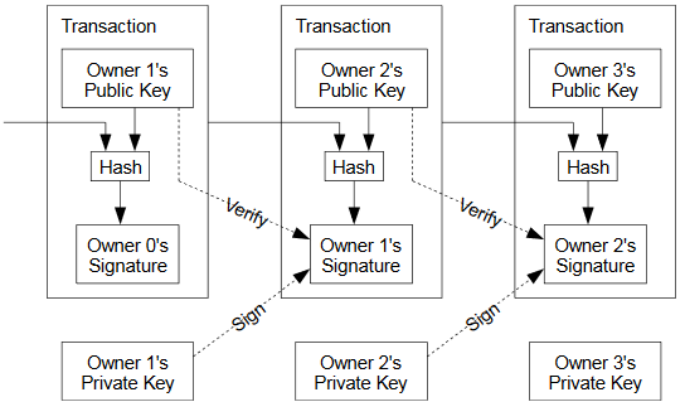


Figura 3. Rappresentazione blockchain nel paper di Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System (2009)

1.2 "Internet del valore"

La tecnologia blockchain oltre ad essere un'alternativa "democratica" agli archivi centralizzati, consentendo dati condivisi, accessibili, distribuiti presso tutti i partecipanti, è parte del concetto rivoluzionario di "internet del valore".

Il punto di partenza è sicuramente il problema della "doppia spesa" o in inglese del *double spending*. I dati su internet viaggiano come copie digitali, il che implica una duplicazione. Quindi, nel caso in cui volessimo scambiare valore tramite internet dovremmo essere certi che gli asset digitali trasferiti fossero unici, poiché il valore risiede nella loro unicità.

Il problema della doppia spesa in un sistema centralizzato, come una banca, viene risolto grazie ad una autorità centrale fidata. In ambito blockchain, il consenso del network evita le doppie spese, consentendole di inaugurare il concetto di "scarsità digitale".

[17] Una funzione crittografica di *hash* converte qualsiasi input (un file mp3, un video, un foglio di calcolo ecc.) in una stringa alfanumerica di dimensioni fisse. Ha tre caratteristiche principali: lo stesso input produce sempre lo stesso output (c.d. *hash*), anche modifiche minime dell'input stravolgono l'output, è una funzione unidirezionale (non esiste un modo per passare dall'*hash* all'input se non provando tutte le combinazioni).

Ciò renderebbe possibile lo scambio istantaneo di valore tra individui, eliminando gli intermediari e i costi delle terze parti normalmente coinvolte nel processo.

1.3 Disintermediazione, Consenso e "Mining"

Alla base del funzionamento di una blockchain pubblica si trova il meccanismo del consenso. Non avendo barriere all'entrata, e non potendo confidare in istituzioni fidate, i nodi del network non si fidano l'uno dell'altro. In un tale contesto, è necessario un processo di governance che porti alla validazione dei blocchi.

Questa situazione è ben esemplificata, nel calcolo distribuito, dal "problema dei generali bizantini"[18]: la difficoltà alla base di questa analogia è garantire l'affidabilità generale di un sistema dove esistono dei nodi difettosi o maligni. Un gruppo di generali circonda una città, devono decidere se attaccare o ritirarsi. Coordinare l'azione è cruciale per evitare che il gruppo si divida e ciò risulti in una sconfitta. Il raggiungimento di una decisione comune è complicato dalla presenza di generali traditori, che possono votare per una strategia subottimale anche in modo selettivo (comunicare ad alcuni generali di volersi ritirare e agli altri di voler attaccare). Inoltre, i voti vengono comunicati tramite messaggeri che potrebbero non arrivare o manipolare i messaggi. La soluzione viene trovata con la combinazione di matematica, teoria dei giochi ed economia all'interno della blockchain.

I nodi che partecipano al processo di consenso sono chiamati *miners*. Il *mining* è il processo attraverso il quale le transazioni vengono validate, riunite in blocchi e poi aggiunte alla blockchain. Il lavoro svolto dal *miner* viene ricompensato secondo le regole del protocollo, solitamente attraverso le commissioni di transazione del blocco e le nuove criptovalute generate.

Esistono diversi algoritmi per la creazione del blocco, i più importanti sono il *Proof of Work ("PoW")* e il *Proof of Stake ("PoS")*.

Il *Proof of Work* è il protocollo utilizzato dalla blockchain Bitcoin. Per aggiungere un blocco, un *miner* si deve adoperare per risolvere un "problema matematico". Ne esistono diverse tipologie: "funzione di *hash"*, i.e. trovare un input da un *hash*, "scomposizione dei numeri primi", ovvero scomporre un numero in due moltiplicatori ecc. La difficoltà del problema influenza l'efficienza e la sicurezza della blockchain, nel caso in cui siano, rispettivamente, troppo difficili o troppo facili[19].

[18] LAMPORT, SHOSTAK, PEASE (1982: 382-401).
[19] TAR (2018).

Il *Proof of Stake* è il protocollo utilizzato dalla blockchain Ethereum. La sua nascita è dovuta alla ricerca di un'alternativa ai grandi consumi energetici propri del PoW. "L'algoritmo Proof Of Stake utilizza un processo di elezione pseudo-casuale per selezionare un nodo che agirà da validatore del blocco successivo"[20]. Al posto della potenza di calcolo posseduta, vengono utilizzati i *tokens*[21]. La dimensione della "stake" (posta, i.e. quantità di *toke*n volontariamente congelati) aumenta le probabilità di essere selezionati come *validator*. Per non favorire solo i nodi più "ricchi" sono impiegati anche altri metodi di selezione. A differenza del PoW, i *forgers*[22] ricevono solamente le commissioni di transazione del blocco.

1.4 Blockchain pubbliche/permissionless e private/permissioned

Le blockchain Bitcoin ed Ethereum sono un modello particolare di blockchain, la c.d. blockchain "pubblica" o *permitionless.* La caratteristica principale risiede nel fatto che non esistono barriere all'entrata, chiunque può prendere parte al network, agire da nodo, analizzare, verificare transazioni e aggiungere blocchi al registro. Non esiste una singola autorità, un "single point of failure". Tutti i nodi sono uguali, nessuna censura. Solitamente, il codice è *open source*, rendendone consultabile il funzionamento. Sicuramente, i punti forti di questo modello sono la decentralizzazione e la trasparenza.

In alcuni settori, però, ciò non è auspicabile, come in ambito industriale. Le blockchain "private" o *permissioned*, fanno dell'efficienza e del controllo sui permessi di accesso la loro priorità, rinunciando alla decentralizzazione. A loro volta si dividono in "completamente private", dove una sola autorità decide quali nodi possono leggere o verificare le transazioni, e *consortium*, dove alcuni nodi vengono considerati degni di fiducia per validare i blocchi. Esistono, inoltre, alcune combinazioni delle due, definite "ibride". Queste distinzioni hanno importanti conseguenze in ambito giuridico e di governance.

[20] ANONIMO (2018).
[21] I tokens sono una rappresentazione digitale di qualsiasi bene o servizio.
[22] Corrispettivo di *miner* su Ethereum.

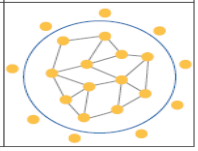
Blockchain type	Explanation	Example	Visualisation
Public permissionless blockchains	In these blockchain systems, everyone can participate in the blockchain's consensus mechanism. Also, everyone worldwide with an internet connection can transact and see the full transaction log.	Bitcoin, Litecoin, Ethereum	
Public permissioned blockchains	These blockchain systems allow everyone with an internet connection to transact and see the blockchain's transaction log, although only a restricted number of nodes can participate in the consensus mechanism.	Ripple, private versions of Ethereum	
Private permissioned blockchains	These blockchain systems restrict both the ability to transact and view the transaction log to only the participating nodes in the system, and the architect or owner of the blockchain system is able to determine who can participate in the blockchain system and which nodes can participate in the consensus mechanism.	Rubix, Hyperledger	
Private permissionless blockchains	These blockchain systems are restricted in who can transact and see the transaction log, although the consensus mechanism is open to anyone.	(Partially) Exonum	

Figura 4- report dello EU Science Hub: Blockchain Now And Tomorrow (2019)

1.5 Limiti della tecnologia blockchain

Il protocollo di consenso garantisce l'immutabilità nelle blockchain pubbliche, ma questo non è vero in assoluto. Anche se improbabile, il sistema può essere compromesso nel caso in cui il 51% dei *miners* si coalizzi per un attacco. Un altro caso è esemplificato dal "The DAO Hack"[23], quando, a seguito di un attacco informatico e al furto di milioni di dollari in criptovalute, la blockchain Ethereum subì una scissione, la c.d. *fork* (precisamente una *hard fork)*. Ciò diede vita a una nuova blockchain ("Ethereum Classic"), dove erano stati disfatti i risultati dell'attacco.

Dal punto di vista della privacy, su cui si tornerà nel quarto capitolo, il Gruppo di lavoro "Articolo 29" ha stabilito che l'*hashing* non è una tecnica di anonimizzazione, bensì di pseudonimizzazione[24]. Infatti, è comunque possibile risalire al soggetto dei dati. Anche per questo motivo, i dati immagazzinati sulla blockchain sono qualificati come "dati personali" ai fini del GDPR, causando non poche frizioni.

Sebbene una delle caratteristiche più rivoluzionarie della blockchain sia la mancanza di fiducia, in quanto la fiducia non è nel network ma nel sistema

[23] GÜÇLÜTÜRK (2018).
[24] Parere del Gruppo di lavoro "Articolo 29" del 10 aprile 2014, Parere 04/2014, *sulle tecniche di anonimizzazione*.

stesso, difficilmente ciò è applicabile quando si passa al concreto, nelle procedure di consenso o nella realizzazione *ex ante* dell'architettura. Quindi, oltre a fidarsi della crittografia e del consenso distribuito, bisogna anche fidarsi dei *miners*, degli sviluppatori e di altri attori fin troppo umani.

Dal punto di vista tecnico, la blockchain Bitcoin, la blockchain pubblica più conosciuta, causa un massiccio consumo di energia e un grande impatto ambientale, è difficile da scalare (lentezza delle transazioni e commissioni elevate) e per via del costo crescente del *mining* (risorse energetiche care e crescente capacità computazionale richiesta) si sono venuti a creare dei *mining pools*, concentrati geograficamente, basati su economie di scala e potenzialmente rischiosi per la governance.

Questi limiti dimostrano che una regolamentazione, più ampia possibile, per esempio a livello europeo, sia auspicabile.

CAPITOLO 2. È POSSIBILE REGOLARE LA BLOCKCHAIN?

2.1 Codice e legge

"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather"[25].

Negli anni Novanta del secolo scorso, la nascita di Internet venne considerata da molti come la premessa di uno spazio (il c.d. "cyberspazio") che si autoregolasse e che si ponesse in contrasto con la territorialità giurisdizionale. Il cyberspazio avrebbe dovuto essere impossibile da regolare. Tuttavia, Internet possiede dei "punti di accesso" attraverso i quali è stato possibile regolarlo, non essendo totalmente decentralizzato. Per esempio, è stato possibile regolare l'e-commerce[26], la protezione dei "dati personali"[27] e l'accesso a "un'Internet aperta"[28].

Con riguardo alla tecnologia blockchain, alcuni sostengono che sia intrinsecamente al riparo dall'interferenza dello Stato, secondo il motto "code is law". Il significato originario di questa espressione[29], riconducibile a Joel Reidenberg e Lawrence Lessig, però, non presume che il codice esautori la legge, sostituendola, ma che il software condizioni normativamente il comportamento degli individui in modo alternativo. Basti pensare all'esempio di Uber: il guidatore che non segue il codice di condotta della piattaforma non viene più preso in considerazione. Il codice non è strumento regolatorio neutro, ma riflette le convinzioni dei suoi sviluppatori. Questo non sfocia, però, nella costituzione di una *lex informatica*, alternativa alla legge, almeno per il momento.

Al contrario, la legge ha un'influenza decisiva sulla formazione del codice[30]. Infatti, molti sviluppatori si sono adeguati a normative esistenti, come nel caso

[25] BARLOW (1996).
[26] Regolamento (UE) del Parlamento Europeo e del Consiglio, del 20 giugno 2019, 2019/1150, *che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online.*
[27] Regolamento (UE) del Parlamento Europeo e del Consiglio, del 27 aprile 2016, 2016/679, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.*
[28] Regolamento (UE) del Parlamento Europeo e del Consiglio, del 25 novembre 2015, 2015/2120, *che stabilisce misure riguardanti l'accesso a un'Internet aperta.*
[29] LESSIG (1999).
[30] FINCK (2019: 40).

del GDPR[31]. Stesso effetto hanno le sentenze. Un caso celebre di come il codice venga influenzato dalla giurisprudenza è il caso *Microsoft Corp. c. Commissione delle Comunità europee*[32]: dopo un'inchiesta cominciata nel dicembre del 1998, la Commissione sanzionò per abuso di posizione dominante il colosso di Redmond. In particolare, per il rifiuto di fornire le informazioni utili a favorire l'interoperabilità e per l'accoppiamento obbligatorio, non rispettoso della concorrenza, del lettore Windows Media Player al sistema operativo Windows[33]. La Commissione previde due linee di azione: costringere Microsoft a rivelare ai concorrenti le interfacce per rendere operabili i server di fascia bassa ma soprattutto fornire una versione di Windows che non includesse Windows Media Player[34]. Con la suddetta sentenza, si confermò ciò che era stato stabilito dalla Commissione, modellando così le nuove versioni del software.

Sebbene il codice possa essere utilizzato per infrangere o aggirare la legge, in molti casi può aiutare ed essere utilizzato per normare il comportamento degli utenti[35]. Alcune funzioni regolatorie sono quindi eseguite da attori privati, come le piattaforme digitali. Un esempio si ha nel caso della domanda di pronuncia pregiudiziale della High Court of Justice (England & Wales), Chancery Division del Regno Unito: *L'Oréal SA e altri c. eBay International AG e altri*[36]. Qui viene sancito che gli organi giurisdizionali nazionali possano "ingiungere al gestore di un mercato online di adottare provvedimenti che contribuiscano, non solo a far cessare le violazioni di tali diritti [tutela dei diritti di proprietà intellettuale] ad opera degli utenti di detto mercato, ma anche a prevenire nuove violazioni della stessa natura"[37].

2.2 Definizione legale

Ai sensi dell'art. 3 del regolamento eIDAS[38], un documento elettronico è un "qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva". Un documento è caratterizzato da

[31] Regolamento (UE) del Parlamento Europeo e del Consiglio, del 27 aprile 2016, 2016/679, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati* (da qui in avanti GDPR).
[32] Sentenza del Tribunale di primo grado (grande sezione) del 17 settembre 2007, causa T-201/04, *Microsoft Corp. c. Commissione delle Comunità europee* (da qui in avanti sentenza del Tribunale di primo grado *Microsoft c. Commissione).*
[33] Sentenza del Tribunale di primo grado *Microsoft c. Commissione*, paragrafi 1031-1090.
[34] Ivi, paragrafi 1222-1229.
[35] FINCK (2019: 41-43).
[36] Sentenza della Corte (grande sezione) del 12 luglio 2011, causa C-324/09, *L'Oréal SA e altri c. eBay International AG e altri* (da qui in avanti sentenza della Corte di giustizia *L'Oréal c. eBay).*
[37] Sentenza della Corte di giustizia *L'Oréal c. eBay*, par. 144.
[38] Regolamento (UE) del Parlamento europeo e del Consiglio, del 23 luglio 2014, 910/2014, *in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.*

tre elementi principali: il mezzo, le informazioni incluse, la caratteristica di essere registrato per permettere a qualcuno di conoscere il proprio contenuto[39]. Le tecnologie basate su registri distribuiti sono strettamente connesse alla concezione più recente di documento, poiché la digitalizzazione ha cambiato uno degli elementi basilari, i.e. il mezzo. In Europa, non esiste una normativa transnazionale che disciplini la tecnologia blockchain, ma alcuni Stati membri hanno preso l'iniziativa. Nel luglio del 2018, una delle prime definizioni delle *Distributed Ledger Tecnology* è stata coniata da Malta. All'art. 2 del suo "Malta Digital Innovation Authority Act", il legislatore definisce le DLT come "a database system in which information is recorded, consensually shared, and synchronised across a network of multiple nodes"[40].

Anche l'Italia, con l'art. 8-*ter* del decreto-legge 135/2018 (convertito in legge 12 del 2019), si pone come uno dei paesi apripista in questo campo. Infatti, viene riconosciuta la validazione temporale elettronica, di cui all'art. 41 del regolamento eIDAS, ai documenti informatici salvati su blockchain. Grazie al *timestamp*, quindi, è possibile conoscere data e ora di registrazione delle informazioni. "Quello che preme sottolineare è che l'Italia, in Europa, è il primo Paese a disciplinare le 'Tecnologie basate su registri distribuiti e smart contract' in coerenza con l'ordinamento comunitario"[41].

Tra le altre realtà che hanno definito legalmente le DLT o le blockchain ci sono: Gibilterra, lo stato dell'Arizona e del Vermont (USA), Bielorussia[42].

2.3 Difficoltà nella regolamentazione

Le caratteristiche intrinseche della blockchain sono sia il motivo della straordinaria attenzione riservatale, sia la ragione per cui una legislazione uniforme sia difficile da raggiungere. Le principali questioni che rallentano l'adozione di cornici normative definite sono: la natura transnazionale, la decentralizzazione, la ricerca di una fonte maggiore di anonimato, monopolio e centralizzazione della governance.

La regolamentazione tradizionale, confinata ai territori nazionali, non riesce a stare al passo con l'aspirazione internazionale delle blockchain distribuite in più giurisdizioni. L'applicazione delle leggi è ugualmente complessa, in quanto un ordine di una giurisdizione potrebbe essere disatteso da un'altra. Inoltre, gli attori coinvolti nel funzionamento di questi registri possono trasferirsi in Stati che combacino maggiormente con le loro preferenze. Ciò accade principalmente per molti nodi, i *miners*, gli sviluppatori e gli intermediari della

[39] SZOSTEK (2019: 37-38).
[40] Atto del governo maltese del luglio 2018, No. XXXI, *Malta Digital Innovation Authority Act.*
[41] NICOTRA, SARZANA DI S. IPPOLITO (2019).
[42] SZOSTEK (2019: 36-44).

blockchain, ma difficilmente per gli utenti finali, ai quali mancano sufficienti incentivi[43]. "In an ideal world, a global blockchain would be regulated by a global regulator"[44].

Dalla natura decentralizzata originaria, un accesso slegato dall'origine geografica, Internet ha cambiato col tempo paradigma, con la nascita della geolocalizzazione e la progressiva centralizzazione. Ciò ha facilitato la regolamentazione[45]. La blockchain, essendo un network *peer-to-peer*[46], difetta di un nodo centrale e gode di livelli maggiori di crittografia. Questo non significa che i server centrali siano gli unici "punti di accesso", come vedremo in seguito. Nella sentenza pregiudiziale della Corte di Giustizia ("CdG"), sul caso *Stichting Brein c. Ziggo BV e XS4All Internet BV*, causa C-610/15, la CdG ha confermato che "The Pirate Bay", un noto sito di *file-sharing peer-to-peer*, potesse essere ritenuto responsabile per violazione del copyright. The Pirate Bay, nonostante le dispute legali, è ancora in attività.

L'anonimizzazione è una questione legata al rispetto del regolamento sul trattamento dei dati personali[47]. Come spiegato in precedenza, il Gruppo di lavoro "Articolo 29" ha stabilito che l'*hashing* non è una tecnica di anonimizzazione, bensì di pseudonimizzazione[48]. Ciò ha un duplice effetto: da un lato, i legislatori hanno un incentivo a favorire lo sviluppo di tecniche di anonimizzazione più avanzate per garantire il rispetto della normativa e facilitare la sua implementazione, dall'altro un eccessivo sviluppo della privacy potrebbe incoraggiare il riciclaggio di denaro o altre attività illecite[49].

Come già elencato nei limiti della blockchain, il *mining* secondo il protocollo di consenso *Proof of Work* è estremamente dispendioso in termini di risorse. Quindi, i più grandi *mining pools* sono stati attratti dai costi economici di paesi come la Cina, che ne ospita il maggior numero[50]. Questa concentrazione di potere non è benefica per il network, anzi pone delle questioni di governance e di monopolio. Finora la maggior parte delle regole che tutelano il network sono informali, come nel caso dei conflitti di interesse.

In conclusione, come Internet ha inaugurato nuove difficoltà nella regolamentazione, per esempio, della protezione intellettuale, "la blockchain introduce un nuovo set di problemi, come ad esempio la legittimità dei diritti di proprietà

---

[43] FINCK (2019: 58-60).
[44] Ivi, p. 59.
[45] Ivi, p. 60.
[46] Rete informatica paritaria, dove i nodi sono sia *client* che *server*.
[47] Regolamento (UE) del Parlamento Europeo e del Consiglio, del 27 aprile 2016, 2016/679, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*.
[48] Parere del Gruppo di lavoro "Articolo 29" del 10 aprile 2014, Parere 04/2014, *sulle tecniche di anonimizzazione*.
[49] FINCK (2019: 63-64).
[50] TUWINER (2020).

di asset fisici registrati su una blockchain pubblica"[51]. Un altro esempio potrebbe essere quello della "eredità digitale"[52], infatti nella materia successoria la decentralizzazione e la conseguente idea che ogni utente sia l'unico responsabile della conservazione dei propri dati, ha già creato situazioni paradossali: alla morte del fondatore di uno degli *exchange* di criptovalute più celebri, né i suoi eredi né i fruitori del sito hanno potuto più accedervi[53].

2.4 Punti di accesso

Nelle infrastrutture centralizzate, la regolamentazione può mirare ad un singolo punto di accesso; d'altra parte, in una infrastruttura decentralizzata, i punti di accesso sono più complicati da definire. Michèle Finck ne suggerisce sei[54]: gli *Internet Service Providers* ("ISP"), i *miners*, i *core software developers*, gli utenti finali, gli intermediari vecchi e nuovi e i governi che partecipano attivamente alla blockchain.

Un network basato sulla blockchain in ultima istanza dipende da Internet. I fornitori di servizi Internet sono stati uno dei punti di accesso privilegiati nel regolare il cyberspazio, poiché facilmente riconoscibili e integrati in una specifica giurisdizione. Infatti, sono stati già sottoposti al regolamento per l'acceso ad "un'Internet aperta", dove all'art. 3 viene consacrato il concetto di "neutralità della rete"[55]. L'intrinseca trasparenza della blockchain pubblica permette agli ISP di risalire ai computer connessi ad un network (tramite indirizzo IP o *hostname*) e in alcuni casi persino analizzare i dati sulla stessa[56]. Tranne nel caso in cui vengano chiusi interi siti, operazione costosa, gli ISP sono normalmente utilizzati per controllare il traffico Internet e bloccare l'accesso degli utenti a siti con contenuti illegali, sebbene utilizzando servizi come VPN o Tor sia possibile evadere la vera posizione geografica, compiendo azioni illegali indisturbati.

I *miners*, il cui compito è aggiungere dati alla blockchain, sono un ulteriore punto d'accesso. Sono facilmente identificabili per tre motivi[57]: innanzitutto, sebbene chiunque possa diventare *miner*, la crescita di calcolo computazionale necessaria per la PoW ha favorito la nascita dei *mining pools*, che sono facilmente tracciabili data il loro alto consumo di energia; ogni qualvolta un nuovo blocco è creato, nuove criptovalute sono destinate all'indirizzo del portafoglio

[51] Position paper dell'Associazione Italiana per la Sicurezza Informatica ("Clusit") del 2019, *Blockchain & Distributed Ledger: aspetti di governance, security e compliance*.
[52] GIACCAGLIA (2019: 950).
[53] ANONIMO (2019).
[54] FINCK (2019: 47-58).
[55] Regolamento (UE) del Parlamento Europeo e del Consiglio, del 25 novembre 2015, 2015/2120, *che stabilisce misure riguardanti l'accesso a un'Internet aperta*.
[56] DE FILIPPI, WRIGHT (2018: 177).
[57] Report tematico dello European Union Blockchain Observatory and Forum del 27 settembre 2019, *Legal and regulatory framework of blockchains and smart contracts*.

virtuale del *miner*; infine, gli ISP possono rintracciare i *miners* nella loro area. I *miners* hanno il potere finale di adottare un nuovo software che modifichi o sostituisca il protocollo precedente, riscrivendo la storia delle transazioni di un database condiviso o aggiungendo ulteriori controlli riguardo all'immagazzinamento, la gestione, la registrazione dei dati[58]. Nell'Unione Europea, i *miners* sono già destinatari di obblighi, per esempio devono rispettare i criteri sulla responsabilità degli intermediari della direttiva sul commercio elettronico[59]. Tuttavia, il trasferimento per una giurisdizione più favorevole è pur sempre un'opzione percorribile in molti casi.

Gli sviluppatori di software hanno la stessa facoltà, ma, nonostante ciò, sono degli ottimi punti di accesso. Di norma sono figure pubbliche, facilmente riconoscibili. Sono responsabili del design, dello sviluppo, della conservazione e dell'evoluzione del protocollo[60]. Sarebbe quindi possibile richiedere di modificare il codice, in modo da consentire l'inserimento di una *backdoor* per supportare più efficacemente l'applicazione delle leggi. Questa soluzione però rischia di minare la sicurezza complessiva del sistema.

La soluzione più diretta per imporre leggi è sugli utenti finali. A differenza di altri attori, non hanno incentivi sufficienti per cambiare la loro posizione. Questo e il fatto che le blockchain pubbliche utilizzino dei metodi di pseudonimizzazione, e non di anonimizzazione, li rendono ragionevoli punti di accesso. Tuttavia, gli utenti tendono a non conoscere i meccanismi che sono alla base della tecnologia, per questa ragione è difficile che influenzino direttamente la governance della blockchain e che siano pienamente consapevoli di tutte le conseguenze delle loro azioni: "imposing liability on individuals for actions that they cannot expect or foresee would lack a sense of fairness and justice"[61]. Un'ulteriore difficoltà è nei numeri elevati degli utenti.

Nonostante le premesse teoriche, la blockchain ha favorito la nascita di nuovi intermediari, come gli *exchange* di criptovalute. Gli intermediari sono ulteriori punti di accesso. Un esempio sono i motori di ricerca, come il caso di pronuncia pregiudiziale *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*[62] che ha permesso l'applicazione del diritto all'oblio del GDPR.

---

[58] DE FILIPPI, WRIGHT (2018: 180).
[59] Direttiva (UE) del Parlamento europeo e del Consiglio, dell'8 giugno 2000, 2000/31/CE, *relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»)*.
[60] Report tematico dello European Union Blockchain Observatory and Forum del 27 settembre 2019, *Legal and regulatory framework of blockchains and smart contracts*.
[61] DE FILIPPI, WRIGHT (2018: 176).
[62] Sentenza della Corte (Grande Sezione) del 13 maggio 2014, causa C-131/12, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González.*

2.5 Esempio della blockchain Bitcoin

La blockchain Bitcoin è esemplificativa di molti aspetti precedentemente trattati. Chiunque può divenire *miner*, scaricare il software e l'intera blockchain, ma questo passaggio costituisce un contratto, concluso online, disponibile ovunque[63]. Il creatore o i creatori del software rimangono anonimi, non si conosce il suo/loro stato di origine, né da quale stato il software sia stato pubblicato. Ciò pone difficoltà per il diritto privato internazionale.

In termini legali, il software è stato fornito secondo la licenza *open-source* MIT, una delle più permissive, in base alla quale è possibile copiare, modificare, distribuire il programma originale o modificato, a condizione che si forniscano informazioni sull'autore[64]. Il fatto che il concessore della licenza sia anonimo non ne mina la validità, difatti il contratto viene eseguito una volta installato il software e i blocchi precedenti[65].

Nel caso del Bitcoin, non è semplice selezionare la legge applicabile per un contratto concluso tra un *miner* e l'autore del software. Nei casi di protezione della proprietà intellettuale, di norma verrebbe applicato il principio di territorialità, la *lex loci protectionis*. Una soluzione potrebbe essere applicare la legge dello Stato in cui la protezione è stata richiesta, ma ciò porterebbe a indicare varie leggi straniere, con le relative difficoltà[66]. Un'altra possibilità è l'applicazione della *lex loci originis* i.e. legge del paese "in which the operation of the given work started online"[67]. Tuttavia, seguendo questa strada, gli utenti sarebbero costretti a rispettare leggi che non conoscono. In futuro, non è da escludere che l'identità dell'autore sia rivelata.

Per qualsiasi contratto concluso da un *miner*, bisogna innanzitutto determinare se sussista la capacità giuridica e capacità di agire. Per fare ciò, necessita trovare il criterio per la legge applicabile. Sono, a seconda degli Stati, criterio della cittadinanza e del luogo di residenza[68].

La scelta della legge applicabile, *a priori*, sarebbe ammissibile, ma la blockchain Bitcoin difetta di tale clausola. Tuttavia, l'art. 3 del regolamento Roma I[69] stabilisce che è possibile scegliere la legge alla conclusione del contratto oppure posteriormente, "in qualsiasi momento". Nel caso in cui non sia stata scelta una legge, all'art. 4 del regolamento Roma I enumera le possibilità. Eppure, con riguardo al contratto tra *miners*, un contratto "innominato" che consiste nella collaborazione tra pari, l'unico criterio possibile da applicare è

[63] SZOSTEK (2019: 64-71).
[64] Ibid.
[65] Ibid.
[66] Ibid.
[67] Ivi, p. 70.
[68] Ivi, p. 73.
[69] Regolamento (CE) del Parlamento europeo e del Consiglio del 17 giugno 2008, 593/2008, *sulla legge applicabile alle obbligazioni contrattuali* (Roma I).

il luogo abituale di residenza. Questo approccio non è esente da svantaggi, come la frammentazione[70].

Un altro problema è la classificazione dell'attività dei *miner*: ai sensi dell'art. 2 della direttiva 2000/31/CE[71], che richiama la direttiva 98/48/CE[72] (art. 1, punto 2) la definizione dei "servizi della società dell'informazione" stabilisce che essi sono "qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi". La remunerazione nella blockchain Bitcoin non è però garantita e nemmeno ricevuta da un'entità terza, è infatti prodotta dal sistema. Inoltre, ciascun *miner*, ai sensi della suddetta direttiva, sarebbe sia "prestatore del servizio" che "destinatario del servizio", poiché oltre a fornire dati, li scarica.

Esistono molti altri temi, come l'arricchimento senza una giusta causa, per esempio nei casi in cui un trasferimento di criptovalute avvenisse per errore o in violazione della legge[73].

In conclusione, sebbene esistano delle difficoltà intrinseche nella natura della blockchain, specialmente di quella Bitcoin, esistono comunque strumenti utilizzabili dai giudici nazionali per i loro giudizi.

[70] SZOSTEK (2019: 77).
[71] Direttiva del Parlamento europeo e del Consiglio dell'8 giugno 2000, 2000/31/CE, *relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»).*
[72] Direttiva del Parlamento europeo e del Consiglio del 20 luglio 1998, 98/48/CE, *relativa ad una modifica della direttiva 98/34/CE che prevede una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche.*
[73] SZOSTEK (2019: 86-87).

3. BLOCKCHAIN, SUPPORTI DUREVOLI E VALUTE VIRTUALI

3.1. La definizione di "supporto durevole"

Negli ultimi anni, la blockchain è stata oggetto di un crescente interesse da parte del settore finanziario e bancario, che risultano essere due delle industrie più attive in questo ambito. Questi settori (e non solo), anche per garantire la conformità normativa, sono interessati alla qualificazione di "supporto durevole", per passare da un modello tradizionale basato su carta a una concezione più moderna di archivio dei dati (per esempio, nei casi di contratti online).

Il termine "supporto durevole" è stato introdotto recentemente nel diritto europeo.

Ai sensi della direttiva 2002/65/CE[74] del 23 settembre 2002, alla lett. f) dell'art. 2, un "supporto durevole" è

> qualsiasi strumento che permetta al consumatore di memorizzare informazioni a lui personalmente dirette in modo che possano essere agevolmente recuperate durante un periodo di tempo adeguato ai fini cui sono destinate le informazioni stesse, e che consenta la riproduzione immutata delle informazioni memorizzate.

Ai sensi della direttiva 2008/48/CE[75] del 23 aprile 2008, alla lett. m) dell'art. 3, un "supporto durevole" è

> ogni strumento che permetta al consumatore di conservare le informazioni che gli sono personalmente indirizzate in modo da potervi accedere in futuro per un periodo di tempo adeguato alle finalità cui esse sono destinate e che permetta la riproduzione identica delle informazioni memorizzate.

Ai sensi della direttiva 2011/83/UE[76] del 25 ottobre 2011, all'art. 2, un "supporto durevole" è

> ogni strumento che permetta al consumatore o al professionista di conservare le informazioni che gli sono personalmente indirizzate in modo da potervi accedere in futuro per un periodo di tempo adeguato alle finalità cui esse sono destinate e che permetta la riproduzione identica delle informazioni memorizzate.

Ai sensi della direttiva (UE) 2015/2366[77] del 25 novembre 2015, al punto 35 dell'art. 4, un "supporto durevole" è

---

[74] Direttiva del Parlamento europeo e del Consiglio del 23 settembre 2002, 2002/65/CE, *concernente la commercializzazione a distanza di servizi finanziari ai consumatori*.
[75] Direttiva del Parlamento europeo e del Consiglio del 23 aprile 2008, 2008/48/CE, *relativa ai contratti di credito ai consumatori*.
[76] Direttiva del Parlamento europeo e del Consiglio del 25 ottobre 2011, 2011/83/UE, *sui diritti dei consumatori.*
[77] Direttiva (UE) del Parlamento europeo e del Consiglio del 25 novembre 2015, 2015/2366, *relativa ai servizi di pagamento nel mercato interno*.

> ogni strumento che permetta all'utente del servizio di pagamento di conservare le informazioni che gli sono personalmente indirizzate in modo da potervi accedere in futuro per un periodo di tempo adeguato alle finalità cui esse sono destinate e che permetta la riproduzione identica delle informazioni memorizzate.

Ai sensi della direttiva (UE) 2016/97[78] del 20 gennaio 2016, al punto 18 dell'art. 2, un "supporto durevole" è

> qualsiasi strumento che: a) permetta al cliente di memorizzare informazioni a lui personalmente dirette, in modo che siano accessibili per la futura consultazione durante un periodo di tempo adeguato ai fini cui sono destinate le informazioni stesse; b) consenta la riproduzione inalterata delle informazioni memorizzate.

Anche la Corte di Giustizia dell'Unione Europea si è interessata alla definizione di "bene durevole": nella sentenza sul rinvio pregiudiziale del caso *Content Services Ltd c. Bundesarbeitskammer* (causa C-49/11[79]) del 5 luglio 2012, la Corte rinvia alle direttive precedentemente analizzate e ad una sentenza della Corte dell'Associazione europea di libero scambio (AELS). Secondo la Corte, un sito web non costituisce un esempio di "supporto durevole", poiché, come scritto al punto 46

> dal fascicolo di causa non risulta che il sito Internet del venditore al quale rinvia il link indicato al consumatore consenta a quest'ultimo di conservare informazioni a lui personalmente dirette in modo da avervi accesso e da poterle riprodurre identiche per un periodo di congrua durata senza che il venditore possa modificarne unilateralmente il contenuto.

Quindi, un sito Internet "le cui informazioni sono accessibili ai consumatori solamente attraverso un link mostrato dal venditore" (punto 50), come quello oggetto del procedimento principale, non può essere considerato un "supporto durevole".

D'altro canto, un sito bancario può essere considerato un "supporto durevole", poiché rispetta i requisiti summenzionati e non permette "qualsiasi modifica unilaterale del suo contenuto da parte del prestatore di servizi di pagamento o da parte di altro professionista cui sia stata affidata la gestione del sito stesso" (punto 44), come si evince dalla sentenza della Corte *Content Services Ltd contro Bundesarbeitskammer* [80]. Inoltre, la Corte si premura di differenziare i termini "fornire" e "rendere disponibile": con il primo che implica che la trasmissione "sia accompagnata da un comportamento attivo del prestatore stesso, destinato a portare a conoscenza dell'utente l'esistenza e la disponibilità di tali informazioni su detto sito".

---

[78] Direttiva (UE) del Parlamento europeo e del Consiglio del 20 gennaio 2016, 2016/97, *sulla distribuzione assicurativa (rifusione).*

[79] Sentenza della Corte (Terza Sezione) del 5 luglio 2012, Causa C-49/11, *Content Services Ltd contro Bundesarbeitskammer*.

[80] Sentenza della Corte (Terza Sezione) del 25 gennaio 2017, Causa C-375/15, *BAWAG PSK Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse AG contro Verein für Konsumenteninformation.*

In conclusione, la legislazione e la giurisprudenza in ambito europeo, riguardo i "supporti durevoli", sono omogenee e consolidate. Le uniche differenze tra le diverse definizioni sono conseguenza dei differenti periodi e della cornice concettuale dell'atto specifico[81]. Ciò permette di isolare le principali caratteristiche di un "supporto durevole": la possibilità di archiviare informazioni, la possibilità di recuperare immutate le informazioni, la possibilità di accedere ai contenuti, senza impedimenti, per un periodo di tempo adeguato al perseguimento degli scopi cui sono finalizzate le informazioni.

3.2. La blockchain è un "supporto durevole"?

Con l'evoluzione della tecnologia, anche la concezione di "supporto durevole" è mutata, come quella di documento. Si è passati da documenti su carta a documenti elettronici, eliminando di fatto la necessità del supporto fisico, come avviene col *cloud storage*. Per quanto riguarda la genesi del documento, nel caso in cui fornirlo sia obbligatorio, ne vengono creati due omologhi per ciascuna parte (la copia e l'originale). Nella blockchain, invece, vige il principio di condivisione dell'informazione. Inoltre, la protezione crittografica sostituisce la firma a mano. La blockchain, quindi, può essere l'ultimo tassello di questa trasformazione[82].

Un esempio proviene dalle banche. Nel caso di revisione dei regolamenti, le banche sono obbligate ad informare i clienti, devono accertarsi che abbiano ricevuto le modifiche e le abbiano lette. Ciascun documento deve essere accessibile per un tempo adeguato, non deve essere rimosso o alterato una volta pubblicato. In teoria, ciò viene reso possibile da un "supporto durevole". Attualmente, la maggior parte delle banche utilizza il proprio sito web o la mail (in casi rari inviano CD-ROM) per pubblicare le revisioni, in modo da risparmiare sulla stampa e i costi di spedizione. Sono però difficili da escludere potenziali manomissioni o perdita di dati[83].

Qui entrerebbe in gioco la blockchain. A questo punto, bisogna però accertarsi che la tecnologia rispetti i requisiti di "supporto durevole". Innanzitutto, bisogna distinguere tra blockchain pubbliche e private[84].

Nelle blockchain private, dove i documenti sono resi accessibili solo ai nodi autorizzati, il rispetto dei requisiti di "supporto durevole" è più agevole. Quando una sola autorità si occupa del registro, allora è l'unica che la gestisce; nel caso di un consorzio, la soluzione migliore è la scelta di più gestori. In questo modo però, i benefici del "non ripudio" e della democratizzazione non saranno applicati.

---

[81] SZOSTEK (2019: 101).
[82] Ivi, p. 103.
[83] SAMCIK (2018).
[84] SZOSTEK (2019: 104-106).

Nelle blockchain pubbliche, essendo i contenuti accessibili a tutti, è possibile pubblicare nei blocchi solamente gli *hash* corrispondenti ai documenti, e immagazzinare gli stessi all'interno di archivi esterni insieme ai propri *hash*. Così che eventuali manipolazioni possano essere rilevate.

Il luogo di archiviazione è quindi un parametro fondamentale per stabilire se la blockchain soddisfi i requisiti di "supporto durevole". Esistono diverse possibilità[85]: il metodo migliore è che tutti i partecipanti al network archivino i documenti, tramite blockchain, nei loro archivi o server; un'altra soluzione è archiviare i dati in un luogo unico (può accadere per esempio in una blockchain privata), tuttavia, ai fini della definizione di "supporto durevole", è preferibile avere più depositi: nel caso di un solo partecipante, seguendo la sentenza *BAWAG PSK Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse AG c. Verein für Konsumenteninformation* [86], è richiesta la presenza di un archivio esterno, per esempio di un fornitore di servizi blockchain terzo; nel caso di un consorzio, con più siti di archiviazione e utilizzo della tecnologia blockchain, i requisiti sono ampiamente rispettati.

L'ultima opzione, non molto pratica ma valida, è che i dati vengano scaricati da tutti coloro che ottengano un documento, con il permesso di accedere ai soli altri file a cui abbiano diritto.

Un altro tema connesso ai "supporti durevoli" è il criterio con cui si registrano le informazioni[87]. Pubblicare l'intero documento tramite tecnologia blockchain, che permette un livello di sicurezza elevato e l'integrità dei dati, risponde ai requisiti. È comunque possibile schedare un documento in uno o più archivi, accostandolo al proprio *hash*, senza salvarlo sulla blockchain. Per mezzo di un registro dati basato sulla blockchain si previene l'eventuale manomissione o rimozione dell'*hash*. Grazie all'*hash* è possibile accertarsi che il documento non sia stato mai modificato da quando pubblicato.

Secondo la definizione di "supporto durevole" e la giurisprudenza in materia, è cruciale che il documento fornito non venga modificato o rimosso per un adeguato periodo di tempo. Sulla blockchain, però, è possibile "dimenticarlo"[88]: ciò accade quando un partecipante non ha più accesso ai dati crittografici necessari alla visione del documento a cui è autorizzato. Per soddisfare i requisiti, quindi, una blockchain deve o escludere la possibilità di un tale avvenimento, oppure deve concedere solo al destinatario del documento di poterlo dimenticare.

---

[85] Ivi, pp. 106-107.
[86] Sentenza della Corte (Terza Sezione) del 25 gennaio 2017, Causa C-375/15, *BAWAG PSK Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse AG c. Verein für Konsumenteninformation.*
[87] SZOSTEK (2019: 107).
[88] Ivi, p. 108.

Un'ulteriore questione è quella del metodo con cui si forniscono le chiavi di accesso[89]. Come scritto in precedenza, nella sentenza *BAWAG PSK Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse AG c. Ve-rein für Konsumenteninformation*, la Corte chiarisce che solo un "comportamento attivo" costituisce un modo corretto di "fornire" informazioni al cliente.

3.3. Valute virtuali nel diritto UE

Le valute virtuali sono parte integrante della tecnologia blockchain. La difficoltà nel normarle proviene dalle loro caratteristiche. Sono entrate nel radar della BCE sin dai loro esordi, incluse le loro potenzialità e i rischi che comportavano. Nel 2012, nel primo report[90] sul tema, dove vengono affrontati sia temi economici che giuridici, la BCE ha definito le valute virtuali come "a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community". Nel secondo report[91] del 2015, la BCE affina la sua analisi, contando più di 500 valute virtuali decentralizzate in circolazione (2014). In aggiunta, il rapporto contiene nuove avvertenze, legate ai rischi connessi alla volatilità dei tassi di cambio, all'anonimia dei beneficiari dei pagamenti e alla mancanza di trasparenza degli investimenti.

Nel 2014, l'Autorità bancaria europea ("ABE"), l'autorità indipendente dell'Unione Europea che si occupa di vigilare sul sistema bancario europeo, nella sua analisi sui rischi derivati dalle valute virtuali[92], specialmente come mezzi di investimento, definisce le stesse come "digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to a FC, but is used by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically". Ricorda inoltre, che nel quadro giuridico dell'Unione Europea, la regolamentazione dei servizi finanziari avviene ai sensi dell'art. 53 (par. 1) del Trattato sul Funzionamento dell'Unione Europea ("TFUE"), riguardante il diritto di stabilimento e di libera circolazione, oppure dell'art. 114 del TFUE, che ha per oggetto il "ravvicinamento delle disposizioni legislative, regolamentari ed amministrative" per il funzionamento del mercato interno.

---

[89] Sentenza della Corte (Terza Sezione) del 25 gennaio 2017, Causa C-375/15, *BAWAG PSK Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse AG c. Verein für Konsumenteninformation.*

[90] Report della Banca Centrale Europea dell'ottobre 2012, *Virtual currency schemes.*

[91] Report della Banca Centrale Europea del febbraio 2015, *Virtual currency schemes – a further analysis.*

[92] Parere dell'Autorità bancaria europea del 4 luglio 2014, *EBA Opinion on 'virtual currencies'.*

Nel 2015, la Corte di Giustizia dell'Unione Europea, nella causa *Skatteverket contro David Hedqvist*.[93], che aveva per oggetto le operazioni di cambio di valute tradizionali nella valuta virtuale bitcoin, ha stabilito che: siccome la valuta bitcoin ha la sola finalità di essere un mezzo di pagamento (punto 24), non può essere considerata come "bene materiale" ai sensi dell'art. 14 della direttiva IVA[94]. Tali azioni, quindi, si qualificano come prestazioni di servizi, ed essendo il bitcoin solo uno strumento di pagamento contrattuale (punto 42), ricadono nelle categorie esenti da IVA.

Nel marzo del 2018, la BCE ha costituito una *Crypto Assets Task Force*, con l'obiettivo di ampliare l'analisi della fenomenologia delle valute virtuali e delle eventuali implicazioni per la stabilità finanziaria dell'Unione[95].

Un'ulteriore definizione la si può trovare nella direttiva (UE) 2018/843[96], che modifica direttiva (UE) 2015/849 (lett. d, punto 18, della modifica dell'art. 3): le valute virtuali sono

> 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.

Recentemente, la necessità di una legislazione europea chiara ed esauriente è stata notata da due enti europei in due documenti separati[97]: il 9 gennaio del 2019, è stato pubblicato un report[98] dell'Autorità bancaria europea, dove si rassicura sui rischi di instabilità finanziaria dovuti alle criptovalute, ma si segnala che alcune criptovalute, non ricadendo nella disciplina dei servizi finanziari, comportano numerosi rischi per il mercato. Lo stesso giorno, l'Autorità europea degli strumenti finanziari e dei mercati ("ESMA")[99], il cui compito è vigilare sui mercati finanziari, ha emesso un report sulle potenziali difficoltà di applicare la regolamentazione dei servizi di investimento a quei *token* qualificabili come "strumenti finanziari". Inoltre, ha suggerito ai legislatori europei di valutare "the opportunity to set up a bespoke regime for those crypto-assets that do not qualify as financial instruments" (punto 182). Non è tuttavia

---

[93] Sentenza della Corte (Quinta Sezione) del 22 ottobre 2015, Causa C-264/14, *Skatteverket contro David Hedqvist*.
[94] Direttiva del Consiglio del 28 novembre 2006, 2006/112/CE, *relativa al sistema comune d'imposta sul valore aggiunto*.
[95] BRACCIALI (2019).
[96] Direttiva (UE) del Parlamento europeo e del Consiglio del 30 maggio 2018, 2018/843, che modifica *la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo.*
[97] LUGANO (2019).
[98] Report dell'Autorità bancaria europea del 9 gennaio 2019, *Report with advice for the European Commission*.
[99] Report dell'Autorità europea degli strumenti finanziari e dei mercati del 9 gennaio 2019, *Advice: Initial Coin Offerings and Crypto-Assets*.

l'intento di questa tesi addentrarsi nell'ambito finanziario. Di seguito, infatti, considereremo la natura delle criptovalute in relazione alla blockchain.

3.4. Profili giuridici delle valute virtuali

È opinione ormai consolidata della BCE, che le valute virtuali non possano essere qualificate come moneta avente corso legale[100]. Anche perché, secondo l'art. 128, par. 1, del TFUE le banconote in euro emesse dalla BCE sono le uniche aventi corso legale in Europa.

Ulteriormente, nel report del 2015 "Virtual currency schemes – a further analysis" già menzionato, la BCE rigetta la tesi secondo la quale le valute virtuali soddisferebbero le tre funzioni tipiche della moneta (mezzo di scambio, riserva di valore, unità di conto) secondo la teoria economica, in quanto sono rispettate solo parzialmente. Infine, non essendo garantite da un'autorità pubblica, come è invece il caso dell'euro, non è obbligatorio accettarle come pagamento dei debiti, e quindi non sarebbero moneta tradizionale neppure sulla base delle teorie "statalistе".

Le valute virtuali non appartengono nemmeno alla specie della moneta elettronica[101]. Difatti, ai sensi dell'art. 2, punto 2, della direttiva 2009/110/CE una moneta elettronica è

> il 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 direttiva 2007/64/CE e che sia accettato da persone fisiche o giuridiche diverse dall'emittente di moneta elettronica.

Tuttavia, le valute virtuali non vengono emesse in cambio di fondi di valore equivalenti in valuta tradizionale. Non danno diritto ad alcun rimborso, né vi è garanzia che vengano accettate come strumento di pagamento. In aggiunta, sono vittime di tassi di cambio volatili e non sono all'interno di un adeguato quadro normativo. Il loro valore e la loro esistenza non sono scindibili dalla tecnologia blockchain.

In aggiunta, non sono qualificabili come "fondi", poiché ai sensi della direttiva (UE) 2015/2366[102], essi si riferiscono solo a "banconote e monete, moneta scritturale o moneta elettronica quale definita all'art. 2, punto 2), della direttiva 2009/110/CE". Da ultimo, secondo la risoluzione del Parlamento europeo

[100] BRACCIALI (2019).
[101] DI VIZIO (2018: 12).
[102] Direttiva (UE) del Parlamento europeo e del Consiglio del 25 novembre 2015, 2015/2366, *relativa ai servizi di pagamento nel mercato interno*.

del 19 aprile 2018 [103] (considerando n. 10), le valute virtuali non vanno confuse né con "valore monetario utilizzato per eseguire operazioni di pagamento", né con le valute di gioco, proprie di ambienti determinati.

3.5. Le valute virtuali come "documento di legittimazione"

Il quadro giuridico delle valute virtuali è certamente complesso. Per comprenderlo meglio, conviene approfondire, all'interno dell'ordinamento italiano, la sostanza dell'accordo che ne è alla base: la blockchain. La valuta virtuale, la cui esistenza è garantita dalla tecnologia, è però anche parte integrante del suo funzionamento.

Come sostenuto in precedenza, la blockchain è un contratto atipico, che deve superare il giudizio di "meritevolezza"[104] pena la nullità. La soglia di meritevolezza sembrerebbe essere superata quando il fine dell'accordo non sia l'utilizzo delle valute virtuali per attività assimilabili a funzioni monetarie o di pagamento, ma invece consenta soprattutto il funzionamento del protocollo[105].

La qualificazione delle valute virtuali non sembra ricadere all'interno dei beni giuridici, sia per le perplessità riguardo la loro immaterialità[106], ma soprattutto per il loro rapporto "simbiotico" con il protocollo blockchain, un potenziale ordinamento alternativo[107].

Perciò, alle valute virtuali non si applicherà la disciplina in materia dei diritti reali, né di circolazione dei beni giuridici ma si adotteranno le norme di origine pattizia derivate dall'accordo istitutivo della blockchain[108].

Le valute virtuali potrebbero essere inquadrate come "documento di legittimazione"[109] del contratto originario, e di conseguenza circolare combinate allo stesso, secondo la disciplina della cessione del contratto[110]. Le regole generali sui contratti si applicheranno a questi documenti informatici di contratti "innominati" (ad esecuzione continuata). Per quanto riguarda la circolazione,

---

[103] Risoluzione legislativa del Parlamento europeo del 19 aprile 2018, *sulla proposta di direttiva del Parlamento europeo e del Consiglio che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo*.
[104] "Le parti possono anche concludere contratti che non appartengano ai tipi aventi una disciplina particolare, purché siano diretti a realizzare interessi meritevoli di tutela secondo l'ordinamento giuridico", ai sensi dell'art. 1322. c.c. (autonomia contrattuale).
[105] LANFRANCHI (2019: 51).
[106] DI VIZIO (2019: 13).
[107] LANFRANCHI (2019: 58).
[108] Ibid.
[109] Art. 2002 c.c.
[110] LANFRANCHI (2019: 59).

essa potrebbe essere non solo l'oggetto del contratto, ma la causa. L'esecuzione del contratto equivarrebbe alla cessione[111].

Tuttavia, questo quadro è solo un mero riconoscimento di alcune caratteristiche delle valute virtuali, e non soddisfa la necessità di una legislazione europea, che punti alla armonizzazione delle normative degli stati membri e garantisca una disciplina che tuteli i diversi interessi in gioco[112].

[111] Ivi, p. 60.
[112] DI VIZIO (2019: 14).

4. GDPR E DATI NON PERSONALI

4.1. Ambito territoriale GDPR e dati personali nel diritto dell'UE

"In their current state DLTs will in most, if not all, instances be incompatible with the GDPR"[113]

La blockchain, in particolare la sua versione pubblica, è una tecnologia che consente di immagazzinare dati e informazioni in maniera condivisa, decentralizzata e immutabile. I dati presenti sulla blockchain sono potenzialmente di ogni tipo: da transazioni finanziarie a cartelle mediche. Il trattamento di informazioni sensibili, personali, è tutelato a livello europeo e ciò comporta delle frizioni che vanno analizzate per garantire lo sviluppo della tecnologia.

Nel dicembre del 2000, la Carta dei diritti fondamentali dell'Unione Europea fu ufficialmente proclamata a Nizza dal Parlamento europeo, dal Consiglio e dalla Commissione. Con l'entrata in vigore del Trattato di Lisbona (2009), la Carta ha assunto la stessa valenza giuridica dei Trattati. All'art. 8, è introdotto il principio della tutela dei dati personali, uno dei diritti che è al centro del dibattito sulle nuove tecnologie e non solo.

In ottemperanza all'art. 16, par. 2, del TFUE, il Parlamento europeo ed il Consiglio hanno deliberato, secondo la procedura legislativa ordinaria, sul trattamento dei dati personali: nel maggio del 2018 il GDPR è diventato vincolante. Si pone un duplice obiettivo: agevolare il libero movimento dei dati personali, preservando i diritti dei cittadini dell'Unione. Questo regolamento, molto ambizioso, si basa sul presupposto che i dati vengano trattati in maniera centralizzata. Da ciò deriva la sua difficoltà nell'interfacciarsi con la tecnologia blockchain, che, nella sua versione pubblica, fa della decentralizzazione il suo cardine.

Sebbene il GDPR sia un regolamento europeo, la sua portata travalica i confini europei. Come stabilito all'art. 3, la sua disciplina si applica indistintamente, nell'ambito di operazioni condotte da uno stabilimento con sede nell'Unione, al "titolare del trattamento" o al "responsabile del trattamento", sia che il trattamento dei dati avvenga all'interno che all'esterno dell'Unione[114]. Nel caso

[113] FINCK (2019: 113).
[114] GDPR, art. 3, par. 1.

di attività che consistano nell'offrire beni o servizi (anche non pagati)[115] oppure quando un comportamento che ha luogo nell'Unione venga monitorato[116], anche il requisito dello stabilimento nell'Unione decade. Infine, quando il "titolare del trattamento" dei dati si sia stabilito in un luogo fuori dall'Unione, che utilizza il diritto di uno Stato membro per il diritto internazionale pubblico, anche qui si applica il GDPR[117].

A causa della natura transazionale della blockchain, è facile assumere che vengano coinvolti Stati terzi e varie giurisdizioni[118]. Ci sono però dei requisiti per i trasferimenti di dati verso paesi terzi o organizzazioni internazionali che sono delineati negli articoli 44-50: i dati possono essere trasferiti sulla base di "una decisione di adeguatezza"[119], di "garanzie adeguate"[120], di "deroghe in specifiche situazioni"[121]. Queste condizioni sono in ordine gerarchico. Il primo requisito da verificare è quindi se la Commissione abbia emesso una decisione di adeguatezza, nel caso in cui la tutela dei dati personali nel paese terzo sia "sostanzialmente equivalente a quello assicurato all'interno dell'Unione"[122]. Qualora non ci sia una decisione di adeguatezza, il trasferimento verso Stati terzi o organizzazioni internazionali può avvenire "solo se ha fornito garanzie adeguate [all'art. 46, par. 2] e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi"[123]. In mancanza delle altre condizioni, ci sono delle specifiche situazioni in cui è autorizzato il trasferimento dei dati. A titolo esemplificativo, il trasferimento è possibile allorquando l'interessato abbia esplicitamente dato il consenso, nonostante sia stato messo al corrente riguardo i rischi[124].

In merito al campo di applicazione materiale, occorre premettere che esistono diversi modi di salvare dati sulla blockchain. Il che ha delle implicazioni in termini di tutela della privacy[125]. Il primo consiste nel lasciare le informazioni così come sono, come *plain text*. Tuttavia, è evidente che ciò permetterebbe a chiunque di leggerle. Inoltre, è possibile fare uso della crittografia, una funzione reversibile, in modo che solo chi sia in possesso della chiave privata

[115] GDPR, art. 3, par. 2 (a).
[116] GDPR, art. 3, par. 2 (b).
[117] GDPR, art. 3, par. 3.
[118] Studio del Panel for the Future of Science and Technology ("STOA") del luglio 2019, *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?* (da qui in avanti Studio del Panel STOA, *Blockchain and the GDPR).*
[119] GDPR, art. 45.
[120] GDPR, art. 46.
[121] GDPR, art. 49.
[122] GDPR, considerando n. 104.
[123] GDPR, art. 46, par. 1.
[124] GDPR, art. 49, par. 1 (a).
[125] FINCK (2019: 90-91).

possa leggere i dati. All'interno di un registro distribuito, la tecnica dell'*hashing*, una funzione irreversibile, permette di trasformare qualunque mole di dati in una stringa alfanumerica dal numero di caratteri predefinito.

Ritornando all'oggetto del GDPR, bisogna chiedersi se le informazioni immagazzinate sulla blockchain si qualifichino come "dati personali". Ai sensi dell'art. 4, par. 1, i dati personali sono

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

Perciò, i dati trattati con tecniche di anonimizzazione ricadono fuori dalle materie di competenza del regolamento. Per dirsi completamente anonimo, però, un dato deve essere elaborato in modo che "irreversibly prevent identification"[126].

Dal punto di vista del GDPR, nessuna delle precedenti procedure di salvataggio dei dati consente di anonimizzare le informazioni[127]. Persino l'*hashing*, un criptaggio "forte", è considerato una tecnica di pseudonimizzazione, non di anonimizzazione[128]. Infatti, la pseudonimizzazione mantiene un legame indiretto tra i dati e "l'interessato", che è possibile palesare utilizzando informazioni aggiuntive[129].

I dati salvati sulla blockchain possono essere di due tipi: "dati transazionali" o chiavi pubbliche. Nel prossimo paragrafo si approfondirà la loro natura e le difficoltà nel sottrarli alla regolamentazione del GDPR.

4.2. Dati "transazionali" e chiavi pubbliche su blockchain

Come accennato in precedenza, sulla blockchain sono presenti due tipi di "dati personali": i dati "transazionali", informazioni connesse alle transazioni (iden-

[126] Parere del Gruppo di lavoro "Articolo 29" del 10 aprile 2014, Parere 04/2014, *sulle tecniche di anonimizzazione* (da qui in avanti Gruppo di lavoro "Articolo 29", *Tecniche di anonimizzazione*).
[127] Report tematico dello European Union Blockchain Observatory and Forum ("EUBOF") del 16 ottobre 2018, *Blockchain and the GDPR* (da qui in avanti Report tematico dello EUBOF, *Blockchain and the GDPR).*
[128] Parere del Gruppo di lavoro "Articolo 29", *Tecniche di anonimizzazione.*
[129] GDPR, art. 4 par. 5.

tità digitali, cartelle cliniche ecc.) e le chiavi pubbliche, stringhe alfanumeriche che, fungendo da indirizzi, permettono la pseudonimizzazione di persone fisiche o giuridiche[130].

Per ciò che riguarda i dati "transazionali", sono a tutti gli effetti "dati personali", nonostante la tecnica dell'*hashing*. Tuttavia, esistono dei casi in cui queste informazioni possano essere sottratte alla disciplina del GDPR[131]. Si può prevedere che in futuro vengano sperimentati nuovi sistemi che consentano la piena anonimizzazione, secondo i criteri delineati dal Gruppo di lavoro "Articolo 29". Al momento, una soluzione potrebbe essere quella di salvare le informazioni *off-chain*, collegandole alla blockchain attraverso un *hash pointer*. In questo modo, i dati immagazzinati sulla blockchain e gli *hash* dei dati *off-chain* sarebbero ancora qualificati come "dati personali", ma sarebbe possibile modificare il database fuori dalla blockchain, secondo i criteri del GDPR. Una delle difficoltà maggiori di questa strada è che richiede un intermediario fidato, privando la tecnologia della sua più promettente qualità. Per questo motivo, sono state sperimentate altre soluzioni *off-chain* decentralizzate. Una delle più promettenti è stata ideata da Jacob Eberhardt e Stefan Tai, consistente in un modello di archiviazione *off-chain* indirizzato per contenuto ("content-addresable storage pattern"[132]). Questo schema è particolarmente efficiente in caso di grandi quantità di dati, consentendo l'utilizzo degli *hash* sulla blockchain per verificare la correttezza delle informazioni archiviate all'esterno.

In relazione alle chiavi pubbliche, non è possibile spostare gli indirizzi *off-chain* ma è possibile offuscarli. Esistono varie tecniche, ognuna con i propri pregi e difetti[133]: uno dei metodi suggeriti è l'utilizzo di indirizzi *stealth*, che consistono in una chiave pubblica monouso, come avviene nella criptovaluta Monero. La criptovaluta Zcash utilizza invece la "zero knowledge proof", che consente di salvare le transazioni sulla blockchain, senza svelarne i dettagli. Ciò avviene attraverso l'uso di risposte binarie di tipo vero/falso. Un'altra tecnica è la "ring signatures", dove la transazione viene firmata da più soggetti. La firma testimonia che il firmatario possiede la chiave privata corrispondente ad una delle chiavi pubbliche di una serie di chiavi, senza palesare quale[134]. Il Gruppo di lavoro "Articolo 29" ha già qualificato come anonimizzazione, se seguita da ulteriori precauzioni riguardo la privacy, la tecnica chiamata "noise

[130] Studio del Panel STOA, *Blockchain and the GDPR*, pp. 26-29.
[131] FINCK (2019: 94-95).
[132] EBERHARDT, TAI (2017: 9-10)
[133] Report tematico dello EUBOF, *Blockchain and the GDPR*, p. 20-24.
[134] BUTERIN (2016).

addition"[135]. In questo caso, le transazioni sono raggruppate, in modo da rendere impossibile il riconoscimento degli individui che le eseguono. Ulteriori tecniche sono in discussione e altre saranno ideate in futuro.

Nonostante ciò, la materia non è stata ancora cristallizzata in giurisprudenza o da linee guida del Comitato europeo per la protezione dei dati[136]. Il che causa non poca incertezza normativa.

4.3. Il controllore dei dati

La questione della responsabilità dei dati è sicuramente il punto focale del GDPR e dipende in gran parte dalla procedura di governance implementata nella specifica blockchain. Tuttavia, la visione centralizzata del regolamento si ripercuote ulteriormente sulla definizione del "titolare del trattamento" (traduzione infelice di *data controller*), inquadrante principalmente i tradizionali modelli *client-server*. Infatti, il "titolare del trattamento" è la persona fisica o giuridica che "determina le finalità e i mezzi del trattamento di dati personali"[137]. Secondo il parere del Gruppo di lavoro "Articolo 29", determinare le finalità e i mezzi equivale a "determinare, rispettivamente, il "perché" e il "come" di certe attività di trattamento"[138].

Sebbene nelle blockchain private sia potenzialmente più facile identificare l'entità che determina i fini e i mezzi, nelle blockchain pubbliche non sono presenti autorità sovraordinate e la governance è più complessa.

La difficoltà nel rintracciare il "titolare" ha favorito la nascita di alcune teorie riguardo alla responsabilità sul trattamento dei dati[139].

Secondo alcuni, i nodi "validatori" potrebbero essere qualificati come *data controllers*. La loro rilevanza nella governance deriva principalmente dal fatto che, in caso di aggiornamento del software, abbiano l'ultima parola, influenzando l'evolversi della piattaforma. Seguendo questa opinione, ciascun nodo dovrebbe essere qualificabile secondo la definizione del GDPR, all'art. 4(7). Quindi, "l'interessato" dovrebbe rivolgersi ai singoli nodi per far valere le obbligazioni nate in virtù del regolamento. I nodi non sono "contitolari del trattamento" (*joint controllers*) ai sensi dell'art. 26(1), poiché non si muovono di concerto per determinare i fini e i mezzi, ma agiscono indipendentemente dagli altri nodi all'interno del sistema. Tuttavia, la contitolarità è possibile in

[135] Parere del Gruppo di lavoro "Articolo 29", *Tecniche di anonimizzazione*, pp. 12-13.
[136] Report tematico dello EUBOF, *Blockchain and the GDPR*, p. 21.
[137] GDPR, art. 4, par. 7.
[138] Parere del Gruppo di lavoro "Articolo 29" del 16 febbraio 2010, Parere 01/2010, *sui concetti di "responsabile del trattamento" e "incaricato del trattamento"*, p. 13.
[139] FINCK (2019: 100-102).

alcune organizzazioni della governance, tra *miners* e sviluppatori o utenti. Ad ogni modo, nel caso in cui fossero identificati come "titolari", le complicazioni sarebbero molteplici[140]: in primo luogo, l'identificazione e la geolocalizzazione di tutti i nodi della rete non è agevole; inoltre, i nodi non hanno accesso alle informazioni decriptate e non sono in grado di modificarle; con riguardo ai casi di effettiva applicazione della legge, moltissimi nodi, anche da più giurisdizioni, dovrebbero essere coinvolti, con la possibilità, in mancanza di alternative, di dover impedire il funzionamento dell'intera blockchain. Un'azione sproporzionata rispetto all'infrangimento dei diritti di un solo *data subject* ("interessato"). Infine, non si comprende come si possano calcolare le multe su una blockchain pubblica ai sensi dell'art. 83, basandosi sul "fatturato mondiale totale annuo"[141].

Nel report tematico riguardante il GDPR, il Blockchain Observatory and Forum suggerisce che gli sviluppatori del protocollo non siano considerati *data controller*[142]. Questo perché lavorano volontariamente ad un software, un mero strumento, che spesso non li remunera direttamente. Perciò, non dovrebbero essere considerati responsabili di come viene utilizzato il loro codice *open source.* Inoltre, viene addotto come esempio il caso paradossale in cui Tim Berners-lee fosse ritenuto responsabile di tutto ciò che avviene sul *World Wide Web*. Sebbene gli sviluppatori siano gli architetti della piattaforma e suggeriscano i vari aggiornamenti, non decidono in merito all'effettiva adozione degli stessi e non influiscono sulle finalità della piattaforma, salvo eccezioni.

A certe condizioni, anche i *data subjects* possono essere qualificati come *data controllers.* Infatti, gli "interessati" possono riacquistare il controllo sui propri dati attraverso la loro chiave privata[143]. Perciò, quando gli utenti aggiungono "dati personali" alla blockchain per scopi commerciali, probabilmente possono essere considerati come "titolari del trattamento"; al contrario, l'inserimento di informazioni personali nell'esercizio "di attività a carattere esclusivamente personale o domestico" ricade invece nell'esenzione di cui all'art. 2(2) del GDPR[144].

Considerando la governance multilivello propria della blockchain, si potrebbe affermare che il "titolare del trattamento" non si trovi al livello infrastrutturale ma a quello delle applicazioni basate su blockchain. Infatti, nella fase iniziale di una tecnologia, gli "interessati" hanno spesso più contatti col piano infrastrutturale, che diminuiscono nella fase di maturità. Proseguendo in questa direzione, l'entità legale che determina i fini e i mezzi a livello delle applicazioni

[140] Ibid.
[141] GDPR, art. 84, par. 6.
[142] Report tematico dello EUBOF, *Blockchain and the GDPR*, p. 18.
[143] FINCK (2019: 101).
[144] Report tematico dello EUBOF, *Blockchain and the GDPR*, p. 18.

va considerata come il *data controller*[145]. È interessante notare che in effetti ciò è già accaduto nel caso dei social network: il Gruppo di lavoro "Articolo 29" ha infatti stabilito che i social network sono "titolari del trattamento" in quanto determinano le finalità e i mezzi del trattamento dei dati. Inoltre, anche i fornitori di applicazioni possono essere considerati *data controllers*, nel caso in cui sviluppino applicazioni, utilizzate dagli utenti, che funzionino in aggiunta a quelle del social network[146].

È plausibile che i nodi, nelle blockchain private, vengano considerati "responsabili del trattamento" (*data processor*) piuttosto che "titolari", in quanto trattano le informazioni "per conto del titolare del trattamento"[147], non determinando né i fini né i mezzi. Un esempio può essere quello di un governo che si affida ad una blockchain: il governo è il *data controller*, i nodi i *data processors*[148].

4.4. Diritti degli interessati rispetto al trattamento dei loro dati personali

Ai sensi dell'art. 12, par. 2, del GDPR, il "titolare del trattamento" ha l'obbligo di agevolare l'esercizio dei "diritti dell'interessato" enumerati dall'art. 15 al 22. In particolare, ci si soffermerà su quei diritti che pongono dei problemi di compatibilità con la tecnologia blockchain.

Innanzitutto, secondo il principio di "minimizzazione dei dati", i dati personali devono essere "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati"[149]. Ciò si pone in diretto contrasto con la natura accrescitiva della tecnologia blockchain. Inoltre, la sua immutabilità complica l'esercizio di altri diritti quali il "diritto di rettifica" e il "diritto all'oblio". Come trattato in precedenza, la tecnica dell'archiviazione *off-chain* potrebbe conciliare l'utilizzo della blockchain con il rispetto di questi diritti, almeno per quanto riguarda i dati "transazionali". La soluzione non è altrettanto immediata con riferimento alle chiavi pubbliche[150].

I dati devono essere "esatti e, se necessario, aggiornati", ai sensi dell'art. 5, par. 1, lett. d). Da qui deriva, che nel caso in cui le informazioni siano datate

[145] Studio del Panel STOA, *Blockchain and the GDPR*, p. 44.
[146] Parere del Gruppo di lavoro "Articolo 29" del 12 giugno 2009, Parere 5/2009, *sui social network on-line.*
[147] GDPR, art. 4, par. 8.
[148] FINCK (2019: 101).
[149] GDPR, art. 5, par. 1(c).
[150] FINCK (2019: 104).

o non corrette, debbano essere rettificate o eliminate dal "titolare del trattamento" nel minor tempo possibile[151]. Quindi, proprio per garantire un tale diritto del *data subject*, il "diritto di rettifica" è previsto all'art. 16 del GDPR. Supponendo che i nodi siano i "titolari", si possono immaginare due ostacoli: in primo luogo, è improbabile che un "interessato" possa identificare i nodi, e anche nel caso in cui riuscisse a rivendicare la rettifica, i nodi non potrebbero modificare i dati[152]. Un dettaglio interessante della disposizione in esame, è che prevede che il "diritto di rettifica" possa essere soddisfatto anche tramite "dichiarazione integrativa"[153]. Ciò potrebbe risolvere l'*impasse* riguardante la modifica dei dati "transazionali". Anche qui, gli indirizzi pubblici non sarebbero modificabili. Strettamente connesso al precedente diritto è l'obbligo di notifica in caso di rettifica o cancellazione dei dati a carico del "titolare"[154]. Perfino in questo caso, l'implementazione sarebbe in teoria molto complicata, se non fosse che l'obbligo decade nel caso in cui la sua riuscita sia "impossibile o implichi uno sforzo sproporzionato"[155].

Il primo diritto del *data subject* ad essere tutelato nel GDPR è il "diritto di accesso". "L'interessato" ha diritto a conoscere numerosi dettagli sul trattamento dei propri dati[156], tra cui: le finalità del trattamento (a), le categorie di dati personali (b), i destinatari (c), il periodo di conservazione dei dati (d), l'esistenza di un processo decisionale automatizzato (h). Il suo esercizio è fondamentale ed è un prerequisito per l'applicazione degli altri diritti[157]. Tuttavia, senza un "titolare del trattamento" regolarmente identificato, anche il "diritto di accesso" si presenta come di difficile applicazione[158]. Quindi, il suo esercizio presuppone una governance trasparente e funzionale, che permetta un'effettiva comunicazione e la gestione dei dati[159].

Uno dei diritti che più si pone in contrasto con le fondamenta, anche ideologiche, della tecnologia blockchain, è sicuramente il "diritto all'oblio". L'art. 17 del GDPR determina i casi in cui "l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo". Le condizioni includono, ma non si limitano a: i dati raccolti non sono più necessari rispetto alle finalità originarie (a), a seguito della revoca del consenso (b), quando vi sia stato un trattamento illecito dei dati (d), a causa di obblighi legali derivati dal diritto dell'Unione o di uno stato membro (e). Ritornando alla distinzione tra dati "transazionali" e chiavi

[151] GDPR, art. 5, par. 1(d).
[152] Report tematico dello EUBOF, *Blockchain and the GDPR*, p. 25.
[153] GDPR, art. 16.
[154] GDPR, art. 19.
[155] Ibid.
[156] GDPR, art. 15, par. 1.
[157] Studio del Panel STOA, *Blockchain and the GDPR*, p. 72.
[158] Report tematico dello EUBOF, *Blockchain and the GDPR*, p. 25.
[159] Studio del Panel STOA, *Blockchain and the GDPR*, p. 72.

pubbliche, si può affermare che le difficoltà maggiori si incontrino nella cancellazione delle seconde[160]. Grazie all'utilizzo dell'archiviazione esterna, sarebbe possibile eliminare i dati necessari, sebbene non ci sia un consenso sul destino degli *hash on-chain.* La questione delle chiavi pubbliche può essere risolta ricordando che il "diritto all'oblio" non è un diritto assoluto. Infatti, la cancellazione può essere subordinata alla considerazione "della tecnologia disponibile e dei costi di attuazione"[161]. Forme alternative e meno categoriche possono essere prese in considerazione perché il termine "cancellazione" non viene definito nel GDPR: alcuni sostengono che l'eliminazione della chiave privata "dell'interessato" sia equivalente alla cancellazione, altri vorrebbero ricorrere a tecniche come il *pruning* o utilizzare i *camaleon hashes*.

La Corte di Giustizia ha già accettato tecniche alternative in questo senso, come la rimozione dall'indice di ricerca nei motori di ricerca all'interno della sentenza *Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*[162] .

4.5. Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

Due principi generali guidano la tutela dei dati personali e sono incastonati nell'art. 25 del GDPR: la protezione dei dati fin dalla progettazione ("by design") e per impostazione predefinita ("by default"). Il primo, descritto nel primo paragrafo, si riferisce agli sviluppatori, agli architetti del sistema che devono rispettare gli articoli del GDPR *ex ante*. Il secondo, fotografato dal secondo paragrafo, prevede che il "titolare del trattamento" metta "in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento" e che "non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica". Sia la struttura dell'architettura, sia l'organizzazione della governance dovranno attenersi ai dettami del GDPR[163].

[160] FINCK (2019: 106-108).
[161] GDPR, art. 17, par. 2.
[162] Sentenza della Corte (Grande Sezione) del 13 maggio 2014, Causa C-131/12, *Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*
[163] Studio del Panel STOA, *Blockchain and the GDPR*, pp. 85-86.

Per ciò che riguarda i dati non personali, non vagano in un vuoto normativo, ma è prevedibile la convergenza futura, grazie a tecniche di *machine learning* sempre più avanzate, con i dati personali[164].

In conclusione, la presenza di incertezza normativa, la difficoltà di applicare il presente regolamento se non a specifiche forme di governance e di architettura, la visione accentrata del GDPR penalizzano questa tecnologia. Tuttavia, se da un lato la regolamentazione di nuovi fenomeni debba aggiornarsi in quanto espressione di una società e di tecnologie datate, dall'altro anche la tecnologia blockchain dovrà indirizzare la sua futura evoluzione all'interno delle cornici normative esistenti. L'immaturità della tecnologia è sicuramente un vantaggio ai fini del futuro incontro tra regolamentazione e blockchain.

[164] FINCK (2019: 93).

5. SMART CONTRACT

5.1. Breve storia degli Smart Contract

Il connubio tra Smart Contract e blockchain è sicuramente una delle tematiche più interessanti che riguarda l'ecosistema delle tecnologie basate su registri distribuiti. La combinazione delle più recenti tecnologie con la sfera dell'economia che si occupa dei servizi giuridici prende il nome di *Legal tech*[165]. Prima di addentrarsi in campo giuridico, è necessario delineare il fenomeno nelle sue caratteristiche essenziali.

Innanzitutto, il termine "contratto intelligente" non nasce con la blockchain. Già negli Anni '90, Nick Szabo, informatico, giurista e crittografo, descrisse il funzionamento degli Smart Contract. Tuttavia, anche se la loro sperimentazione risale a quegli anni, i "contratti intelligenti" sono stati concepiti a metà degli Anni '70. Non è una novità l'utilizzo delle tecnologie emergenti per la conclusione di contratti. In passato (ma ancora oggi), l'EDI ("Electronic Data Interchange") ha permesso la comunicazione tra computer di diverse organizzazioni, attraverso lo scambio di documenti standardizzati di business. Eppure, questo interscambio di dati non si avvale dell'utilizzo di algoritmi o di protocolli "intelligenti", permette semplicemente una più efficace e rapida conclusione dei contratti tradizionali[166]. In seguito, si sperimentarono i contratti "data-oriented", espressione di istruzioni contrattuali comprensibili ai computer, all'interno di una connessione macchina-macchina.

Con l'avvento degli Smart Contract, il rapporto tra contratti e tecnologia ha ricevuto un'ulteriore spinta. Nel 1994, Szabo definisce gli Smart Contract come "computerized transaction protocol that executes the terms of a contract"[167]. Questi contratti ingloberebbero tutte le fasi contrattuali, riducendo al minimo l'interferenza esterna degli intermediari[168]. L'intenzione è quella di tradurre o trasporre in codice le tipiche clausole contrattuali, in modo che sia impossibile o eccessivamente costoso violare il contratto. Ciò è reso possibile dalla logica Booleana, che segue lo schema "if-this-then-that", cioè all'avverarsi di una condizione (*if*), segue necessariamente un risultato (*then*). Concepite le clausole, il software elabora in modo deterministico i dati, senza lasciare spazio all'interpretazione. La coesistenza all'interno degli Smart Contracts di tecniche crittografiche, protocolli automatizzati con interfacce utenti

[165] GAROFALO (2019: 872).
[166] SZOSTEK (2019: 111).
[167] SZABO (1994).
[168] SZABO (1997).

semplificate e l'esecuzione automatica del contratto (una volta soddisfatte certe condizioni), ha attirato l'attenzione anche di molti non addetti ai lavori.

5.2. Blockchain e Smart Contract

La vera difficoltà è che, quindi, la fiducia è giocoforza nel codice e nei dati che sono la fonte del processo[169]. Se ad un *input* segue indiscutibilmente un *output*, allora i dati immessi devono essere integri, affidabili e impossibili (o difficili) da manipolare. Inoltre, queste fonti di dati devono essere correttamente controllabili e leggibili. Infine, il codice dello Smart Contract stesso deve essere impossibile da modificare. Anche qui, ritorna la figura di garanzia terza, solitamente un notaio o un avvocato, per sopperire al problema della fiducia. Proseguendo su questa strada, però, l'intenzione stessa alla base di questa innovazione verrebbe meno.

È qui che entra in gioco la blockchain. Il successivo livello di sviluppo della tecnologia. Le caratteristiche della blockchain, come l'irrevocabilità del salvataggio degli Smart Contract sulla stessa, la sua protezione crittografica di alto livello e l'auto-esecuzione, risolvono la questione della mancanza di fiducia. Come affermato in precedenza, la fiducia non è più in un ente sovraordinato, ma nel sistema. Il Bitcoin è un esempio conosciuto di Smart Contract.

Esistono numerose definizioni, non uniformi. Spesso, le spiegazioni differiscono anche in relazione al campo di appartenenza degli esperti che li definiscono: molti informatici tendono a considerare i "contratti intelligenti" come alternativi ai contratti tradizionali, frutto della cosiddetta *lex informatica*; per molti avvocati, invece, essi non rientrano nel ciberspazio ma altro non sono che mezzi e non accordi in sé[170]. Il report[171] (citato più volte) dello UK Government Chief Scientific Adviser li definisce così: "Smart contracts are contracts whose terms are recorded in a computer language instead of legal language. Smart contracts can be automatically executed by a computing system, such as a suitable distributed ledger system".

In definitiva, è possibile tratteggiare le caratteristiche essenziali degli Smart Contract: sono scritti in linguaggio informatico, sono auto-eseguibili o hanno

[169] BELLINI (2018).
[170] SZOSTEK (2019:117).
[171] Un report dello UK Government Chief Scientific Adviser del dicembre 2015 (pubblicato nel gennaio 2016), *Distributed Ledger Technology: beyond block chain*.

un meccanismo di esecuzione automatica, possono essere salvati sulla blockchain (non è necessario), contengono clausole contrattuali.

5.3. Definizione legale degli Smart contract

La sperimentazione degli Smart Contract non è passata inosservata. Tuttavia, i legislatori europei non hanno ritenuto i tempi maturi per una eventuale regolamentazione tradizionale, poiché la tecnologia è in una fase ancora non definitiva. Stringere le maglie della legge in questo stadio potrebbe impedire lo sviluppo spontaneo della tecnologia. È altrettanto vero, però, che un'eccessiva incertezza normativa potrebbe avere il medesimo effetto. La soluzione è nel mezzo, come spesso accade.

L'Unione europea ha elaborato, per mezzo delle sue istituzioni e iniziative, dei documenti riguardanti le questioni giuridiche che gli Smart Contract pongono. Il primo documento è il paper[172] della Banca Centrale Europea, il cui autore è Phoebus Athanassiou, dove gli Smart Contract vengono definiti come

> 'contractual-type' arrangements embedded in software, which the latter can validate, execute and record automatically, on a DLT platform, as soon as certain pre-programmed conditions, agreed upon by human agents, have been met, based on information fed into the DLT itself or received from a pre-defined (mostly external) source.

Il secondo è la risoluzione[173] del Parlamento europeo del 3 ottobre 2018. L'organo elettivo dell'Unione "sottolinea" che gli Smart Contract possano essere funzionali alle applicazioni decentralizzate, quindi spinge la Commissione a investigare le problematiche giuridiche e le potenzialità derivanti dalla loro implementazione. Inoltre, il Parlamento "sottolinea" che al fine di promuovere l'utilizzo degli stessi è necessario raggiungere la certezza normativa sull'utilizzo della firma digitale crittografata e infine "invita" nuovamente la Commissione a favorire lo sviluppo di norme standardizzate nelle relative organizzazioni internazionali.

Il terzo è il report tematico[174] dello European Union Blockchain Observatory & Forum (iniziativa della Commissione europea) del 27 settembre 2019: nel rapporto vengono analizzate questioni relative sia alla blockchain e agli Smart

[172] Paper della Banca Centrale Europea dell'11 Ottobre 2017, *Impact of digital innovation on the processing of electronic payments and contracting: an overview of legal risks*.
[173] Risoluzione del Parlamento Europeo del 3 Ottobre 2018, P8_TA-PROV (2018)0373, *Distributed ledger technologies and blockchains: building trust with disintermediation*.
[174] Report tematico dello European Union Blockchain Observatory and Forum del 27 settembre 2019, *Legal and regulatory framework of blockchains and smart contracts*.

Contract, sia vengono suggerite delle linee guida per la regolamentazione. Innanzitutto, si distinguono gli "Smart Legal Contract", i "contratti intelligenti" espressione di contratti legali, dagli "Smart contract with legal implications", nuove realtà che hanno indiscutibilmente implicazioni legali. Per ciò che riguarda i primi, vengono evidenziati le questioni dei requisiti formali (propri dei diversi ordinamenti degli Stati membri), dei requisiti per le firme digitali dettati dal regolamento eIDAS e la necessità di un "Qualified Trust Service Provider", dell'immutabilità degli Smart Contract, dei controlli/ispezioni di qualità, della effettiva efficacia nel mondo "reale" degli Smart Contract. I secondi, invece, comprendono i "contratti intelligenti" che rappresentano asset digitali, che costituiscono organizzazioni autonome decentralizzate, che si fanno agenti autonomi. In conclusione, vengono suggeriti otto principi per regolamentare la tecnologia blockchain e gli Smart Contract.

Per sopperire alla mancanza di disposizioni in ambito Smart Contract, alcune definizioni degli stessi sono state coniate dai singoli Stati: l'emendamento allo statuto 44, capitolo 26, dello Stato dell'Arizona, dove viene inserito all'interno dell'art. 5; l'annesso n°1 sul Development of Digital Economy del decreto del Presidente della Repubblica di Bielorussia n°8 del 21 dicembre 2017; infine, la definizione di Smart Contract contenuta all'interno del Malta Digital Innovation Authority Act C901 e nel Virtual Financial Asset Act C778 è considerata una delle più valide e vale la pena di essere riportata:

> "Smart contract" means a form of innovative technology arrangement consisting of:(a) a computer protocol; and, or(b) an agreement concluded wholly or partly in an electronic form which is automatable and enforceable by execution of computer code, although some parts may require human input and control and which may be also enforceable by ordinary legal methods or by a mixture of both[175].

Anche l'Italia ha definito gli Smart Contracts, seppur con delle improprietà linguistiche. Infatti, il legislatore italiano tende a confondere gli Smart Contract con il contratto di cui all'art. 1321 c.c. (ipotesi vera solo in caso di contratto stipulato direttamente sotto forma di codice). Essendo un modello consensuale, ed essendo i consensi previamente scambiati, sorgono dubbi sul suo carattere automaticamente vincolante che esiste dal momento della sua esecuzione. Inoltre, anche se l'obbligatorietà derivasse dal suo carattere immutabile, il legislatore non avrebbe considerato che esistono diversi tipi di DLT, non tutte pubbliche[176].

[175] Atto del governo maltese del luglio 2018, No. XXXI, *Malta Digital Innovation Authority Act*.
[176] GIACCAGLIA (2019: 954).

5.4. Smart contracts nell'area del contratto?

Il primo quesito che viene da porsi quando si approfondisce il profilo giuridico degli Smart Contract è capire se debbano essere collocati nell'area del contratto o meno. Secondo alcuni, i "contratti intelligenti" dovrebbero essere in quell'area per essere regolati, mentre altri, sempre di avviso positivo, credono nella categoria dei "legal Smart Contracts", che contenendo l'accordo sarebbero i contratti stessi. Coloro che sono contrari credono, invece, che gli Smart Contract non siano altro che mezzi per la conclusione degli accordi. Altri ancora avvertono che se considerassimo gli Smart Contract dei contratti essi stessi, ogni errore non sarebbe controllabile dall'esterno perché ormai parte del contratto[177].

La soluzione potrebbe trovarsi nel fatto che queste alternative sembrino parziali. Infatti, analizzando a monte i diversi tipi di Smart Contract, è possibile dividerli in due categorie: gli accordi effettivi, portati a termine online tramite consenso (spesso scaricando un software) e "auto-eseguibili", che possono essere considerati propriamente Smart Contract (ad esempio l'accordo tra *miners* nel Bitcoin); i mezzi, che sono espressione di accordi precedentemente stipulati in modo tradizionale ed eseguiti automaticamente dal software, che non meritano tale qualificazione. Quindi, ciò che determina la natura di uno Smart Contract è contenuto nello stesso o nell'accordo originario[178].

Una volta appurato quali siano gli Smart Contract è possibile analizzarli più efficacemente. Gli elementi strutturali del contratto, l'accordo delle parti, oggetto, causa e forma ai sensi dell'art. 1325 c.c., non costituiscono un ostacolo all'implementazione degli Smart Contract. Infatti, "l'intelligenza" del contratto non è sinonimo di intelligenza artificiale ma di accelerazione nella conclusione dell'accordo. Il contratto ha sempre la propria fonte nell'accordo tra le parti. Per quanto riguarda la causa e l'oggetto, rimane inalterato il loro significato. Il requisito della forma scritta, come definito nel Decreto Legislativo n. 135/2018, è soddisfatto pienamente dal codice, senza alcuna discriminazione rispetto alla forma cartacea[179].

Gli Smart Contract si prefiggono obiettivi molto ambiziosi, come impedire alla radice la possibilità d'inadempimento, ma sono affetti da alcune problematiche che rischiano di limitare il progresso della loro applicazione. Nel

[177] Ivi, p. 956.
[178] SZOSTEK (2019: 117).
[179] GAROFALO (2019: 872).

prossimo paragrafo si affrontano alcuni di questi problemi, tuttavia senza la sicurezza di conoscere anche le risposte.

5.5. Alcuni problemi relativi all'utilizzo degli Smart Contract e le frizioni con l'ordinamento giuridico

Come intuito nel precedente paragrafo, le competenze informatiche diventano quindi un prerequisito per la conclusione degli Smart Contract. La prima osservazione che ne consegue è che si generino delle differenze tra il contraente ignaro delle meccaniche dietro il codice e quello esperto in informatica. Una situazione che ricorda gli Anni Sessanta, negli Stati Uniti e in Australia, e il dibattito sul *Legal English* e la *Plain Language*[180].

Di conseguenza, nonostante uno dei pregi degli Smart Contract sia la disintermediazione, la costruzione diventa più complessa. Per la conclusione di un accordo, per esempio, sono necessarie diverse figure professionali: il responsabile dell'iniziativa, lo sviluppatore del software, l'operatore di piattaforma che comunicherà con l'utilizzatore[181]. Saranno inoltre necessari giuristi qualificati, che siano in grado di affiancare gli esperti di informatica, anche per tradurre concetti come "buona fede", "ragionevolezza" ecc. Un altro fenomeno che probabilmente sarà fondamentale nel futuro è "l'ibridizzazione della figura professionale"[182]: le competenze tecniche saranno imprescindibili. Nel caso in cui vengano consultati degli intermediari, per esempio tradurre in codice il contratto, si genereranno delle responsabilità, la cui portata non è ancora chiara.

Una delle problematiche più gravide di conseguenze è sicuramente l'immodificabilità e l'irrevocabilità degli Smart Contract. Sebbene l'esecuzione automatica del contratto e la sua integrità siano due degli aspetti che più spingono all'implementazione di questa tecnologia, sono anche la principale causa delle diffidenze riguardo la stessa. La difficoltà di controllo esterno da parte dei contraenti e dell'ordinamento impedisce anche il naturale svolgimento della funzione giudiziaria. Nel momento in cui il programma è in auto-esecuzione, non è più possibile modificare o cessare la sua applicazione, anche qualora sia legittimo. Sebbene sia possibile fare ricorso agli organi giudiziari *ex post*, alcune situazioni non sono reversibili. Per ovviare a tale inconveniente, alcuni sviluppatori stanno ideando delle funzioni di auto-distruzione del programma,

[180] DELFINI (2019: 176).
[181] PARDOLESI, DAVOLA (2019: 9).
[182] GAROFALO (2019: 873).

la possibilità di interferire sulla sua esecuzione. Le autorità giudiziarie valutano, invece, modalità alternative di intervento[183].

Nel diritto del lavoro, che si riconosce nell'appianare le differenze tra contraenti, la parità sostanziale e formale di situazioni giuridico-patrimoniali tra le parti, presunta dai "contratti intelligenti", sembra rendere più difficoltosa la compatibilità tra blockchain e rapporti di lavoro[184].

Infine, le difficoltà relative alla legge applicabile e al giudice territorialmente competente sono le stesse della blockchain[185].

Queste sono alcune delle problematiche degli Smart Contracts.

[183] GIACCAGLIA (2019: 958-960).
[184] GAROFALO (2019: 874).
[185] Position paper dell'Associazione Italiana per la Sicurezza Informatica ("Clusit") del 2019, *Blockchain & Distributed Ledger: aspetti di governance, security e compliance*.

CONCLUSIONE

L'obiettivo di questa tesi è, dopo aver spiegato in termini essenziali la tecnologia, inquadrare giuridicamente il fenomeno della blockchain e degli Smart Contract all'interno del contesto europeo, far emergere i punti di frizione tra la tecnologia e il diritto dell'Unione Europea, ed evidenziare alcuni ambiti in cui la regolamentazione è più carente.

Come è facilmente intuibile, le potenzialità della tecnologia blockchain e degli Smart Contract sono notevoli. Tuttavia, non sono esenti da criticità, che non possono essere risolte se non con un approccio ampio e lungimirante. La differenziazione e il divario fra le normative dei diversi Stati membri dell'Unione Europea, quando presenti, non è uno scenario promettente e rischia di creare rilevanti disparità economiche e sociali.

Per suggerire una legislazione che non sia nemica dell'innovazione, è interessante riprendere in considerazione il report tematico[186] dello European Union Blockchain Observatory and Forum e le sue conclusioni.

La prima riguarda la necessità da parte dei legislatori europei di definire, in modo ampio, chiaro e semplice, la blockchain e gli Smart Contract, in modo da costituire una cornice condivisa.

Nella seconda conclusione viene evidenziato che, una volta raggiunta un'interpretazione legale della tecnologia, è importante che sia comunicata alle altre autorità nazionali e a livello europeo.

La terza distingue tre strade per regolamentare la blockchain: applicare le leggi attuali, che (come argomentato nella tesi) rischia di creare un regime di incertezza normativa nel quale la tecnologia sia confinata in una fase di immaturità e negando parte del suo potenziale; utilizzare i casi studio per emendare pragmaticamente le leggi, a costo di generare delle falle nel caso in cui non si consideri lo sguardo d'insieme; creare nuove regole, che siano specifiche per ciascun caso d'uso ma che rischiano di entrare in contrasto tra loro, data anche la velocità con cui la tecnologia si rinnova. Non esiste una strategia corretta in ogni occasione ma bisogna conoscere pregi e difetti di ciascuna via.

[186] Report tematico dello European Union Blockchain Observatory and Forum del 27 settembre 2019, *Legal and regulatory framework of blockchains and smart contract*.

La quarta tratta, anche per via del carattere transnazionale della blockchain, il tema dell'armonizzazione delle normative sulla tecnologia in ambito europeo e dell'auspicata omogeneità delle interpretazioni.

Nella quinta conclusione viene chiarito che l'educazione dei *policy makers*, attraverso esperienze dirette e concrete della tecnologia, sia vitale per una legislazione consapevole.

La sesta è incentrata sull'importanza di riconoscere i casi d'uso più urgenti e con alta priorità, quelli che hanno maggiore impatto nel breve termine, come gli asset digitali e il GDPR.

La settima consiglia di impiegare l'approccio *wait-and-see* negli ambiti in cui la tecnologia sia ancora immatura, promuovendo l'auto-regolamentazione.

L'ultima conclusione riprende l'educazione dei legislatori, ma stavolta insiste sull'utilizzo della blockchain come strumento di regolamentazione, per "sporcarsi le mani".

BIBLIOGRAFIA

ANONIMO (2019), *Bitcoin: morto uno dei pionieri, 150milioni in fumo. Nessuno sa la password,* in Novà del "il Sole 24 Ore", reperibile *online*;

ANONIMO (2019), *Quali iniziative UE a supporto della Blockchain?*, in Blockchain4Innovation, reperibile *online*;

ANONIMO (2018), *Proof of Stake*, in Binance Academy, reperibile *online*;

BARLOW (1996), *A Declaration of the Independence of Cyberspace,* in Electronic Frontier Foundation, reperibile *online*;

BELLINI (2020), *Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia*, in Blockchain4Innovation, reperibile *online*;

BRACCIALI (2019), *Cripto valute: la Banca Centrale Europea è chiamata a prendere misure concrete verso l'emissione della propria valuta digitale*, in Diritto Bancario, reperibile *online*;

BUTERIN (2016), *Privacy on the blockchain*, in Ethereum Blog, reperibile *online*;

CARRIÈRE (2019), *Possibili approcci regolatori al fenomeno dei crypto-asset; note a margine del documento di consultazione della Consob*, in *Diritto bancario*, reperibile *online*;

CASTELLANI, TRIBERTI, POMI, TURATO (2019), *blockchain. Guida pratica tecnico giuridica all'uso*, Firenze;

CHIAP, RANALLI, BIANCHI (2019), *Blockchain: tecnologia e applicazioni per il business*, Milano;

DE FILIPPI, WRIGHT (2018), *Blockchain and the Law: The Rule of Code*, Harvard;

DELFINI (2019), *Blockchain, Smart Contract e innovazione tecnologica: l'informatica e il diritto dei contratti*, in *Rivista di diritto privato*, pp. 167-178;

DI VIZIO (2019), *Lo statuto giuridico delle valute virtuali: le discipline e i controlli. Tra oro digitale ed ircocervo indomito*, in *Fondazionepesenti.it*, reperibile *online*;

EBERHARDT, TAI (2017), *On or Off the Blockchain? Insights on Off-Chaining Computation and Data,* in ResearchGate, reperibile *online*;

FINCK (2019), *Blockchain Regulation and Governance in Europe,* Cambridge;

GAROFALO (2019), *Blockchain, smart contract e machine learning: alla prova del diritto del lavoro*, in *Il lavoro nella giurisprudenza*, vol. 27 fasc. 10, pp. 869-880;

GIACCAGLIA (2019), *Considerazioni su Blockchain e smart contracts (oltre le criptovalute)* in *Contratto e impresa*, 3/2019, pp. 941-970;

GÜÇLÜTÜRK (2018), *The DAO Hack Explained: Unfortunate Take-off of Smart Contracts,* in Medium, reperibile *online*;

LAMPORT, SHOSTAK, PEASE (1982), *The Byzantine Generals Problem*, in *ACM Transactions on Programming Languages and Systems*, vol. 4, n. 3 pp. 382-401;

LANFRANCHI (2019), *Profili giuridici delle valute virtuali,* in *Cyberspazio e diritto,* vol.20, n. 62 (1-2-2019), pp. 43-64;

LESSIG (1999), *Code and Other Laws of Cyberspace,* New York;

LUGANO (2019), *EBA ed ESMA chiedono regole comuni sulle crypto,* in Cryptonomist, reperibile *online*;

NAKAMOTO (2009), *Bitcoin: A Peer-to-Peer Electronic Cash System*, in Bitcoin.org, reperibile *online*;

NICOTRA, SARZANA DI S.IPPOLITO (2019), *Al via la blockchain revolution: ecco cosa potremo fare grazie alla nuova norma*, in Agenda Digitale, reperibile *online*;

PAGLIERY (2013), *FBI shuts down online drug market Silk Road*, in CNN Business, reperibile *online*;

PALETTA (2019), *Impatti sulle valute virtuali dal recepimento della V Direttiva antiriciclaggio,* in Diritto 24 ne Il Sole 24 Ore, reperibile *online*;

PARDOLESI, DAVOLA (2019), *"Smart contract": lusinghe ed equivoci dell'innovazione purchessia,* in *IL FORO ITALIANO*, fasc. 4 (Aprile 2019), pp. 195-207;

PARKER (2017), *European Commission 'actively monitoring' Blockchain developments*, in Brave New Coin, reperibile *online*;

SAMCIK (2018), *Durable media on blockchain. It will affect us all*, in subiektywnie o finansach, reperibile *online* (tradotto);

SZOSTEK (2019), *Blockchain and the law*, Baden-Baden;

TAR (2018), *Proof-of-Work, spiegata semplicemente, in* Cointelegraph, reperibile *online*;

TUWINER (2020), *Bitcoin Mining Pools*, in Buy Bitcoin Worldwide, reperibile *online*;

VELLA (2019), *Distributed Ledger Technology: definizione e caratteristiche*, in Osservatori Digital Innovation, reperibile *online*.

ABSTRACT

This thesis deals with the implications of legal uncertainty linked to blockchain and Smart Contracts in European Union law. Eleven years have passed, since the first global application of blockchain technology was implemented: the bitcoin. From that moment, in every industry (in particular, the finance sector) there has been an intense competition among different firms in order to find new fields of application for that technology. Then, once the blockchain interested an increasing number of private actors, Governments and other public players decided to discover new ways of leveraging the technology and, in some cases, they have intervened with new legislation. In this scenario, the European Union, through its institutions and its initiatives, has adopted a "wait-and-see" strategy. It consists of a careful observation of technology development and of the application of existing legal framework. As a matter of fact, considering the stage of the technology at the time, it is safe to assume that the production of new legislation could have hindered its progress. The crucial initiatives, set in motion by the Commission to gain knowledge about the technology, were: the EU Blockchain Observatory and Forum, launched in February 2018, the purpose of which is to increase the velocity of blockchain innovation and spread the blockchain network within the European union. To achieve its goals, it focuses its efforts on analysing the barriers to adoption of blockchain, on sharing common competences and good practises and other activities; the European Blockchain Partnership ("EBI"), created in April 2018 , which entails that the signatories of this declaration will cooperate with the intention of deepening the understanding of this emerging technology and of realising the European Blockchain Services Infrastructure ("EBSI"), which will allow the development of blockchain-based public services within the EU. Another relevant initiative is the resolution by the European Parliament in 2018 *building trust with disintermediation*, in which many blockchain applications are listed and guidelines are defined in order to make the European Union a major player in this area. More recently, Member States and European institutions have ushered a period of "regulatory cooperation". Today, however, it has become clear that the "wait-and-see" approach is no longer viable, because of the numerous frictions and uncertainties connected to blockchain regulation.

The first chapter is dedicated to the blockchain and its functioning. Blockchain is not a synonym of distributed ledger technologies and as it is for other complex technologies, the comprehension of the mechanism behind this innovation is preparatory to analyse the legal aspects of the subject. However, blockchain is not only about technology, because it carries ideological and cultural underpinnings too. The idea behind this technology is linked to anarchic roots and at its core there is the mistrust towards the central power of the state. It is no coincidence, that blockchain is an alternative to centralized storage of data. In fact, one of the crucial concepts related to blockchain is trust. In the past,

trusted intermediaries, such as banks, were the only ones allowed to store information because of their credibility. With the arrival of blockchain, this pattern is challenged by the concept of a decentralized storage of data, in which the trust is in the system and not in a trusted third party involved in a transaction, for example. In order to be considered as an alternative, blockchain faces the "double spending" problem. This issue is related to digital assets. On the web, data travel around the world as digital copies, which implies duplication. In the case of value exchange, uniqueness is the most important characteristic and blockchain proved to be capable of guaranteeing it. Digital scarcity is the premise of the "internet of value". Once analysed the theory, it is time to consider the technology itself. As written above, a blockchain allows a decentralized storage of data. Its architecture is made up of a chain of blocks which contains digital pieces of information. Every block is linked with the following through cryptography. This particular database in append-only, so that it keeps an entire history of all the transactions. The most interesting characteristics of blockchain technology are transparency, immutability and decentralization. As already stated, blockchain disrupts the way we think about trust. To validate a block, which contains information, a governance process is needed. This mechanism is known as "consensus algorithm" and it allows the coordination between parties that do not trust each other. Another important distinction is between public blockchains and private blockchains. The end of the chapter is dedicated to the limits of blockchain.

The second chapter sets out the connection between code and law, provides some examples of States that elaborated definitions of blockchain and illustrates the issue of regulating an emerging and complex technology like this one. It is safe to maintain that the difficulties in regulating DLTs are inherent in their nature. Their transnational character, the decentralized method of data storage, their ambition for a greater level of anonymity and finally the problems linked to power concentration and monopoly. Their cross-judicial aspiration makes the research for the applicable law burdensome, leads to legal uncertainty, favours illegal activities etc. Therefore, a multilateral cooperation would guarantee solid foundation and would foster DLTs development. Decentralization, through peer-to-peer networks, devoid of a single point of failure, hinders the possibility of low-cost law enforcement and again it makes difficult for the judge to apply laws. Anonymity is strictly connected with GDPR compliancy, since at the moment the majority of blockchain are qualified as pseudonymous networks and to be compliant it is necessary to foster the development of anonymization techniques, but this must not result in favouring illegal activities by loosening law enforcement. Last but not least, since mining within the proof-of-work framework (adopted by Bitcoin) has been becoming increasingly expensive, miners have gathered in "mining pools" which could lead to power concentration, when talking about governance. An evident example are the mining pools in China. a consequence of its decentralization Regulating permitionless blockchains can be challenging.

Trough an analogy, the internet regulation, it is possible to find the more efficient modalities and the most promising regulatory access points. Internet Service Providers (ISPs) have been used for internet regulation, because of their specific jurisdiction and easy identification. Internet traffic can be managed, nodes identified. However, there are drawbacks, such as the fact that contents remain available because only user access is blocked etc. Miners are easily identifiable (for example those who have gathered in a mining pools), are already recipients of legal obligations and they can be subject to new regulation or economic incentives to shape the network. The influence on the network mainly depends on the decentralisation. Core software developers are responsible for the architecture of the blockchain system and they can suggest updates that are ideal to introduce specific features. The mobility of "core devs" must be considered. End users' mobility is improbable (low incentives), this makes them an interesting access point. Even if they cannot often affect directly blockchain governance, they can be enforcers of regulation. Old intermediaries, such as search engines, and new ones, such as cryptoasset exchanges, are valid access points. Even Governments are interested in joining blockchain governance, create their own blockchains etc. Finally, the Bitcoin example is displayed.

The concept of "durable media" and an analysis of the legal framework for virtual currency are presented in the second chapter. In the last few years, blockchain has attracted a growing number of sectors, particularly fintech. This sector, the most active in this field, is interested in the definition of "durable media", to guarantee regulatory compliance and to switch from a traditional paper-based model to a more modern one (e.g. online contracts). In the definition of "durable media" three requirements are essential: the possibility of storing information, the guarantee of data integrity and the possibility to access contents for an appropriate period of time related to data purposes. Consequently, blockchain could be the next step of "durable media" evolution. Then, it is explained under what conditions a blockchain can be considered a "durable media". Even in this case, the distinction between private blockchains and public blockchain is relevant. When it comes to virtual currencies, the complexity of blockchain is reflected on their nature. After having introduced virtual currencies, through the definitions of EU institutions, it is showed why they cannot be qualified as legal tender, traditional money, electronic money, "funds", etc. Focusing on the Italian legal framework, it is suggested a possible qualification of virtual currencies as "documents of legitimation".

The fourth chapter is about the frictions between the GDPR regulation and the blockchain. This technology, especially its public version, allows the storage of information in a shared, decentralized and immutable way. Data recorded can vary from financial transaction to medical records. This personal information is protected under EU law. The regulation (EU) 2016/679 of the Euro-

pean Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data was developed for a centralized vision of storing data, therefore it poses serious difficulties when combined with a decentralized mechanism of data management (DLT). At this stage, the majority of distributed ledger technologies are not compliant with the GDPR, so it is crucial to understand the frictions between the two. First of all, it should be clear the distinction between two types of data present on a DLT: "transactional data" and public keys. The former relates to transactions, the latter is a string of letters and numbers, useful for pseudonymous identification. Both are personal data under the GDPR definition. As pointed out by European Parliamentary Research Service, "the GDPR is built on the principle that responsibility and accountability rest with the controller, who is charged with the practical effectiveness of European data protection law"[187]. But when it comes to public blockchains, determining the data controller could be controversial. According to article 3 GDPR, the territorial scope of the regulation is limited to data controllers or processors established within the EU, without considering where the data is processed. Another important issue is the compliancy with rights of data subjects (data minimization, the right to amend, the right to access, the right to be forgotten). GDPR ensures data protection by design and by default, DLTs must take it into account from the beginning.

Smart Contracts are the other topic, related to implementation of blockchain technologies, that are debated in the fifth chapter. After a brief history of online agreements, the legal dimension of Smart Contracts is taken under consideration. It is not straightforward. Problems also arise regarding anonymity, the irreversibility of self-execution and the possibility for the judge to intervene only afterwards. Global Smart Contracts, for actors in different legal systems, functioning in cyberspace are a challenge. Smart Contracts are defined in a report by the UK Government Chief Scientific Adviser as "contracts whose terms are recorded in a computer language instead of legal language. Smart contracts can be automatically executed by a computing system, such as a suitable distributed ledger system"[188]. The definitions are not uniform but there are some fundamental characteristics: are recorded in programming code with contractual clauses, automated method of execution, sometimes recorded in a blockchain, irrevocability. The possibility that smart contracts could be considered in the context of contracts is considered. The nature of a smart contract is linked to the context in which it is used. There are two types of smart contracts: an actual agreement concluded entirely online, through its

[187]A study by the Panel for the Future of Science and Technology ("STOA") of July 2019, *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?*

[188]A report by the UK Government Chief Scientific Adviser of december 2015 (published in January 2016), *Distributed Ledger Technology: beyond block chain*.

acceptance, and a way of recording an agreement concluded before in a traditional way. They do not function in a legal vacuum and they must comply with standard legal requirements such as legal capacity.

In conclusion, it is evident that blockchain technology and Smart Contracs have a great potentiality. However, their innovative character can come to light only under a certain legal framework, in which all their complexity and their frictions with EU law are resolved. A wide and forward-looking approach is required. The discrepancy among different legislations of Member States, in the field of blockchain, is discouraging. As a matter of fact, this scenario could lead to economic and social disparities in the EU, in the long term. This is the reason why, an EU-wide regulation is desirable, as explained in the eight conclusions of the thematic report *Legal and regulatory framework of blockchains and smart contract* of the European Union Blockchain Observatory and Forum.