Alma Mater Studiorum
Università di Bologna

SCUOLA DI ECONOMIA, MANAGEMENT E STATISTICA

-Sede di Forlì-

Corso di Laurea Magistrale in

Economia e Management

Classe LM-77 – Scienze Economico-Aziendali

TESI DI LAUREA

in

DIRITTO D'IMPRESA AVANZATO

TITOLO

SMART CONTRACT E BLOCKCHAIN: ASPETTI NORMATIVI DOMESTICI E INTERNAZIONALI

CANDIDATO:

Michele Carfora

N° matricola: 0000843345

RELATORE:

Professor

Marco Tupponi

Anno Accademico 2018/2019

18 Febbraio 2020

Sommario

INTRODUZIONE

Negli ultimi anni è stato evidenziato l'impatto rivoluzionario della Blockchain che, a prescindere dalle criticità che ne caratterizzano l'attuale fase di sviluppo, costituisce senza dubbio un fattore innovativo in grado di incidere sugli assetti politici, economici e sociali esistenti.

Quando si parla di Blockchain si identifica espressamente, secondo la definizione tradizionale accolta a livello globale, «un database aperto e distribuito in grado di registrare transazioni in modo efficiente, verificabile e permanente».

Dunque, "La Blockchain è una tecnologia che permette la creazione e gestione di un grande database distribuito per la gestione di transazioni condivisibili tra più nodi di una rete." Questa definizione si riferisce, quindi, a un database strutturato in blocchi tra loro collegati, ciascuno dei quali contiene più transazioni, che sono validate dalla rete stessa nell'analisi che viene fatta di ciascun blocco. Ogni nodo della catena è costituito fisicamente dal server attraverso il quale ciascun partecipante ha accesso alla blockchain, vede, controlla e approva tutte le transazioni. Per altri, invece, la blockchain esprime al meglio l'evoluzione del concetto di "ledger" ossia di "libro mastro".

Prima dell'avvento della blockchain, in relazione ai sistemi che già consentivano lo scambio di transazioni e informazioni, era prevalente il concetto di logica centralizzata, nella quale tutto faceva riferimento ed era gestito da una singola unità o autorità, della quale i soggetti avevano fiducia. Con il concetto di decentralized ledger si assiste a un fenomeno di decentralizzazione dell'informazione: essa non è più custodita da un'unica unità centrale, ma si sposta nelle periferie, che assumono sempre più rilevanza nella transazione. La vera innovazione, però, è rappresentata dal passaggio dal concetto di "decentralized ledger" a quello di "distributed ledger": questo è il punto che più caratterizza l'avvento della tecnologia blockchain.

Il concetto di un libro mastro distribuito in copie uguali di informazioni a una moltitudine di persone (chiunque possegga una chiave criptografica può partecipare a una blockchain pubblica) consente di evolversi in una nuova logica di governance, un nuovo contesto in cui non esiste più la possibilità che prevalga un'unità sulle altre (come le autorità centrali su quelle locali). La logica primaria diventa invece quella della fiducia tra tutti i soggetti: il processo decisionale passa attraverso la costruzione del consenso tra tutti i partecipanti, ognuno dei quali ha le stesse informazioni degli altri.

È il 1991 quando Stuart Haber e Walter Scott Stornetta lavorano alla prima catena di blocchi protetta da crittografia. Nel 1992 gli stessi Haber e Stornetta, incorporano i Markle tree (struttura schematica ad albero) alla blockchain, realizzando così un miglioramento dell'efficienza del sistema nel raccogliere più documenti in un unico blocco. Dal 1993 al 2008 la tecnologia blockchain rimane solo un'idea ipotetica di difficile applicazione: il potenziale era già chiaro ma l'applicazione pratica restava ancora un'incognita.

La prima Blockchain fu distribuita ed elaborata nel 2008 da una persona o un gruppo di persone anonime che si sono attribuite il nome di Satoshi Nakamoto. L'anno seguente è stata implementata come componente principale della valuta bitcoin e con la funzione di libro mastro contenente tutte le informazioni pubbliche delle transazioni.

Tuttavia, pur essendo senza dubbio una tecnologia dalle prospettive interessanti, la Blockchain può essere ancora definita di frontiera, con un numero limitato di casi applicativi e diverse incertezze sul quadro legislativo di contorno. C'è una particolare area della Blockchain che è in uno stadio ancora più sperimentale: quella degli Smart Contract. Affinché uno Smart Contract funzioni è indispensabile il consenso tra le parti. Ma nonostante tutta la fiducia possibile tra gli interlocutori, per il regolare funzionamento degli Smart Contract risulta indispensabile la presenza di un intermediario che ne garantisca l'affidabilità e impedisca possibili manomissioni. L'alternativa è rappresentata dall'inserimento, quindi, di una procedura automatizzata che si sostituisca a questo intermediario, garantendo l'immutabilità e l'affidabilità degli Smart Contract. Questa funzione può, oggi, essere assolta dall'applicazione della tecnologia Blockchain.

Alla luce delle osservazioni esposte, dunque, il presente studio, che si articola in tre parti, intende offrire un quadro d'insieme dei principali elementi e caratteristiche di questa complessa struttura dati, condivisa e immutabile.

Nel primo capitolo, dopo aver illustrato la genesi, la definizione e il funzionamento, si passano a rassegna le diverse tipologie di blockchain. Successivamente, particolare enfasi viene posta sul fenomeno delle valute virtuali: si analizza come nasce e si sviluppa una criptovaluta e il suo difficoltoso meccanismo di funzionamento.

Il secondo capitolo contiene un approfondimento sul tema degli smart contracts, o contratti intelligenti, divenuti il fulcro di numerosi dibattiti in materia di trasformazione digitale, per gli svariati contesti in cui possono trovare applicazione, e perché

rappresentano una delle molteplici dimensioni del crescente fenomeno della blockchain. La caratteristica di tale contratto è che le parti raggiungono un accordo sulle clausole e sui tempi sfruttando la logica del "if-this- then-that", ossia se si verifica un presupposto (this) allora consegue un risultato (that); per il resto il contratto intelligente ha la capacità di far rispettare le proprie condizioni ed entrare in esecuzione senza il supporto di una parte esterna. Proseguendo, poi, nella disamina si confronta lo smart contract con il contratto tradizionale.

Nel terzo, ed ultimo, capitolo, si sposta il focus sui profili giuridici. In particolare, viene tratteggiata un'analisi comparata nel panorama internazionale, evidenziando come in alcuni Stati sono state emanate delle legislazioni o delle proposte di legge che ne riconoscono già valore, mentre altri Stati hanno posto in essere delle task force che sono volte principalmente allo studio degli impatti e delle possibilità applicative.

CAPITOLO I

LA TECNOLOGIA BLOCKCHAIN: UN NUOVO PARADIGMA NEL SISTEMA ECONOMICO E SOCIALE

1.1 Premessa

"La tecnologia che probabilmente avrà l'impatto maggiore, nei prossimi decenni, è arrivata. E non sono le reti sociali, non sono i cosiddetti "big data", non è la robotica, non è l'intelligenza artificiale, vi stupirà che si tratta della tecnologia alla base delle monete digitali, come Bitcoin…"

Parole tratte da un discorso di uno dei massimi esponenti in questa materia, Don Tapscott, in un TED[1] (Technology Entertainment Design), un concetto ben articolato e confutato all'interno di uno dei sui libri[2]. Punto di partenza volto a sottolineare l'importanza di tale tecnologia, capace di rivoluzionare il modo in cui si interagisce e si commercia, di creare un paradigma diverso da tutti quelli esistenti, ossia in grado di creare un nuovo modo di trasferire valore. Per capire tale concetto bisogna, in prima analisi, dare una corretta e approfondita spiegazione di cos'è la Blockchain, come funziona, le sue applicazioni e i vari cambiamenti che può apportare in molti settori, per poi delineare i suoi vantaggi. Tutto ciò per poter dare un quadro generale all'oggetto principale di quest'elaborato: gli smart contracts. Essi rappresentano l'aspetto più interessante di questo processo evolutivo tecnologico, ovvero un protocollo che permette a due individui di stipulare un contratto senza un ente terzo che vigili (notaio, funzionario di Stato, ente giuridico). Lo scopo è quello di fornire strumenti per comprendere il singolare fenomeno, affrontando anche le

[1] TED è un'organizzazione no profit dedita alla diffusione di idee, generalmente sotto forma di brevi e potenti discorsi (18 minuti o meno). TED è iniziato nel 1984 come una conferenza in cui convergevano tecnologia, intrattenimento e design e oggi copre quasi tutti gli argomenti - dalla scienza al mondo degli affari a questioni globali - in oltre 100 lingue. Nel frattempo, organizzare eventi TEDx in modo indipendente aiuta a condividere idee nelle comunità di tutto il mondo. (da: https://www.ted.com/about/our-organization).

[2] Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World, Paperback – June 12, 2018.

diverse questioni giuridiche che ruotano intorno a questi argomenti. Dunque, partendo dalle origini, viene effettuata un'analisi della tecnologia Blockchain.

1.2 La genesi della *Blockchain*

Nel 2008 l'industria finanziaria è andata in banca rotta e, forse a suo vantaggio, una persona anonima (o un collettivo) di nome Satoshi Nakatomo, pubblicò un saggio[3] in cui sviluppa un protocollo per una moneta digitale, che utilizzava una criptovaluta sottostante chiamata Bitcoin. Questa criptovaluta consente di effettuare transazioni senza bisogno di un intermediario, e questo atto, apparentemente semplice, ha innescato una scintilla capace di rivoluzionare il mondo. La stessa figura, intorno alla quale aleggia un enorme mistero, sembra che abbia iniziato a lavorare al codice circa un anno e mezzo prima della pubblicazione del famoso paper: "*sto lavorando a un nuovo sistema di denaro elettronico completamente da pari a pari, senza necessità di una terza parte fidata*"[4], diceva in un suo intervento originale già nel Novembre 2008. Oggi è universalmente noto come il padre del Bitcoin. Dal 19 Novembre 2009 fino alla fine del 2010 ha effettuato 575 post su *Bitcointalk*[5], più precisamente fino al 2 Dicembre, data in cui ha deciso di interrompere le sue uscite pubbliche. L'unica apparizione successiva sembra essere avvenuta il 7 Marzo del 2014, un semplice *"I am not Dorian Nakamoto"*, al fine di smentire la caccia mediatica all'omonimo nippoamericano che, secondo il settimanale "Newsweek", poteva essere identificato come il vero autore del Bitcoin.[6] Rilevante è la data 9 gennaio 2009, in cui il Bitcoin è stato rilasciato per la prima volta su *SourceForge*[7]. Infatti, attraverso una modalità di rilascio "*Open Source"*[8], il software è verificabile e migliorabile da

[3] Satoshi Nakatomo, "*Bitcoin: A peer-to-Peer Electronic Cash System",* 2008 (https://bitcoin.org/bitcoin.pdf).
[4] Satoshi Nakamoto, *Cryptography Mailing List*, 1° novembre 2008, intervento originale disponibile qui: www.mail-archive.com/search?l=cryptography%40metzdowd.com&q=subject:%22Bitcoin+P2P+e%5C-cash+paper%22&0-oldest &f=1.
[5] Forum relativo ai Bitcoin, sito ufficiale disponibile al seguente indirizzo: https://bitcointalk.org/index.php.
[6] De Collibus F. M., Mauro R., "*Hacking Finance – la rivoluzione del bitcoin e della blockchain*", Milano, Agenzia X, 2016.
[7] Piattaforma e sito web che fornisce gli strumenti per portare avanti un progetto di sviluppo software in modo collaborativo (open source) tra gli sviluppatori. Sito disponibile all'indirizzo: https://sourceforge.net.
[8] Letteralmente "sorgente aperta", ovvero la possibilità di accedere in modo legittimo e gratuito a costrutti intellettuali, come codice sorgente, prodotti da terzi, eventualmente implementandoli e redistribuendo le modifiche entro i limiti della licenza d'uso con la quale l'autore originale ce li ha forniti. Non esistono segreti: la cucina è aperta, chiunque può vedere come stiamo cucinando, con quali ingredienti, ed

chiunque, di conseguenza è possibile perfezionarlo, risolvendo al contempo in modo rapido bug e problemi che la comunità stessa contribuisce a scoprire. Ciò che al contrario non è previsto per il codice sorgente o proprietario.

Dunque, agli inizi del 1992 un gruppo di persone iniziò ad incontrarsi sistematicamente, con cadenza mensile, negli uffici della Cygnus Solutions, l'azienda di Gilmore nell'area della baia di San Francisco, per discutere di varie materie. Discussioni che spaziavano dalla matematica alla crittografia, dall'informatica alla politica e alla filosofia, fino a tematiche sociali di quel periodo. Il gruppo, che venne battezzato da uno dei suoi membri con il nome di "Cypherpunk", diede vita ad un movimento che in due anni arrivò ad avere 700 iscritti. Basta soffermarsi sulla genesi del nome per avere una prima idea dei suoi principi su cui si basa. Infatti, *cypher* è una parola inglese che sta per cifrario, ovvero colui che scrive codici come si utilizza nella crittografia, mentre punk indica quella corrente di pensiero degli anni '80. Secondo quest'ultima, le autorità centrali avrebbero leso le libertà fondamentali degli individui tramite il controllo operato sulle transazioni e sullo scambio di informazioni. Avversa quindi, all'egemonia dei governi, delle banche e del "sistema" generalmente inteso. I primi esponenti Eric Hughes, Timothy C.May e John Gilmore e in seguito i successivi attivisti, comunicavano attraverso una mailing list, chiamata appunto *Cypherpunk miling list.* Luogo in cui fu pubblicato il Manifesto firmato Heric Hugles del 3 Marzo 1993, che così inizia:

"Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world. […]".[9]

Espressione che riassume la volontà di un movimento di rivendica e chiarimento del concetto di privacy e sicurezza, ormai di puro dominio delle autorità centrali non solo da un punto di vista di conoscenza ma anche di gestione. In seguito continua:

"We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence. […]"[10]. In definitiva quindi, la crittografia può rappresentare un mezzo per ottenere la propria libertà personale.

eventualmente usare i fornelli per darci una mano. (De Collibus F. M., Mauro R., "*Hacking Finance – la rivoluzione del bitcoin e della blockchain*", Milano, Agenzia X, 2016).

[9] Documento disponibile all'indirizzo: https://www.activism.net/cypherpunk/manifesto.html.

[10] Si veda nota 9.

Il primo invece che ebbe l'idea di creare una moneta virtuale fu Wei Dai, descritta in un documento chiamato "*b-money, an anonymous, distribuited electronic cash system*" e pubblicato appunto nella mailing list cypherpunk. L'idea di fondo era che con la creazione di una moneta digitale si intendeva evitare ogni forma di intermediazione nell'esecuzione dei pagamenti[11]. Infatti, all'interno del documento viene elaborato un modello anonimo di transazioni basato su due concetti:

- creazione di moneta attraverso la crittografia;
- registrazione e pubblicazione delle transazioni da parte di un gruppo di utenti che fungevano da server, cosicché tutti i partecipanti avessero la possibilità di controllare la certezza della registrazione.

Nel documento infatti si può leggere: *"in both cases I will assume the existence of an untraceable network, where senders and receivers are identified only by digital pseudonyms (i.e. public keys) and every messages is signed by its sender and encrypted to its receiver"*[12]. Un Sistema che precede il concetto di registro distribuito, fondato sulla crittografia e che consente la diffusione di ogni informazione sulle transazioni a tutti i suoi partecipanti.

Aspetto peculiare di questa parentesi storica è la volontà di sottolineare un paradigma, dal quale si partirà per comprendere la forza dirompente della Blockchain e quindi, il perché si ritiene che sia la più rivoluzionaria degli ultimi tempi. Di fatto, tra tutte le recenti innovazioni tecnologiche, quella più studiata, combattuta e controversa è senza dubbio la Blockchain. Non a caso è oggetto anche di quest'elaborato, il quale mira a dare però una diversa chiave di lettura del fenomeno. L'intento è di partire prendendo in considerazione il seguente paradigma: sicurezza – istituzioni – centralizzazione, che a sua volta necessita di qualche riferimento storico prima di essere chiarito.

Gli economisti hanno studiato il comportamento umano per centinaia di anni: come si prendono decisioni, quali comportamenti adottano in un gruppo, come si scambia valore. Hanno studiato le istituzioni che regolano i commerci, come i sistemi giuridici, società e mercati. Il tutto per arrivare ad un sunto principale, ovvero che esiste una relazione tale per cui l'essere umano in quanto tale, per scambiare valore, necessita di ridurre le proprie incertezze. Per sentirsi più sicuri sentono il bisogno di affidarsi a qualcuno o a qualcosa, appunto un'istituzione. Uno dei primi, in economia ad esplorare questa idea di istituzioni

[11] Mancini N., "*Bitcoin rischi e difficoltà normative"*, in Banca Impresa e Società, p.112, 2016.
[12] Dai W., *B-Money*, in http://www.weidai.com/bmoney.txt, 1998.

come strumenti dell'economia è il premio Nobel Douglas North, il quale riteneva che le stesse sono il lubrificante che permette agli ingranaggi dell'economia di funzionare[13], cosa che si può osservare nel corso della storia umana. Istituzioni intese non solo come ente o organo (istituzioni formali), ma anche come regola o consuetudine (istituzioni informali), tutte fissate fin dai tempi preistorici pur di garantire un ordine volto a facilitare qualsiasi attività economica. Col passare del tempo infatti, man mano che le società si evolvevano e diventavano sempre più complesse, si è avuto un passaggio da istituzioni formali a quelle informali, dove le seconde erano a supporto o a superamento delle prime. Si parla della nascita degli organismi pubblici, delle banche, degli enti economici come le società per azioni, istituzioni che hanno aiutato a gestire i commerci quando le incertezze e le complicazioni continuavano a crescere a fronte di quanto detto prima. Ciò che emerge è che il perno principale del paradigma è l'istituzione, creata e rafforzata proporzionalmente al crescere dell'insicurezza dell'essere umano. Sicurezza invece, che a sua volta diventa sinonimo di istituzione. Chiarito questo aspetto, manca un ultimo tassello, che è la netta conseguenza di un legame così stringente: il controllo personale sia sui propri dati e sia sulle transazioni diminuiva. In poche parole, per la premura e l'attenzione verso un senso di sicurezza le persone hanno accettato ma soprattutto ceduto, direttamente e in molti casi indirettamente, i propri dati. Si è perso il controllo sulla propria identità, intesa come insieme dei dati relativi ad un soggetto, a vantaggio di un terzo incuranti delle conseguenze. Con questo non si vuole affermare che da un giorno all'altro le persone abbiano affidato la propria identità generosamente, o che l'intermediario, cioè l'istituzione, abbia approfittato di tale possesso. Semplicemente da un lato c'è la volontà di sentirsi sicuri quindi ci si affida ad un terzo, dall'altro c'è l'intermediario che possiede le loro identità per garantire un corretto funzionamento degli scambi. Il punto è che, trovandosi a gestire una moltitudine di dati riguardanti sia i soggetti e sia le loro transazioni, l'istituzione diventa necessariamente l'unico mezzo per effettuare un qualsiasi tipo di connessione o scambio. Tutto questo ci porta alla fine, che riassunto in un'unica parola, si chiama centralizzazione. Un paradigma che, in qualsiasi prospettiva venga visto o analizzato vede come perno principale l'istituzione, ma soprattutto è espressione di un motore che permette il funzionamento dell'attuale società.

[13] North C. D., "*Istituzioni, cambiamento istituzionale, evoluzione dell'economia"*, Il Mulino, 27 maggio 1994.

Tenendo in considerazione il fenomeno Cypherpunk, non come fenomeno isolato, ma come parte di un processo evolutivo, si può notare la forza di voler andare oltre a questo sistema risale a tempi ancora più lontani. Si pensi ad internet per esempio, nato per dare la possibilità a tutti di essere in collegamento, ma a seguito della sua affermazione non si è fatto altro che trasferire le istituzioni al suo interno, costruendo piattaforme che gestiscono l'identità, a questo punto virtuale. Banche, governi e perfino piattaforme di mercato come Amazon o eBay, intermediari più veloci che facilitano le attività economiche umane. Internet, la democrazia dell'informazione[14], non è riuscita ad andare oltre questo schema. Questo perché inviando attraverso la rete un file, mail o altro, in realtà si sta trasferendo una copia. Mentre subentra il problema quando si tratta di inviare una proprietà, come il denaro, risorse finanziarie, proprietà intellettuale, arte e cioè una transazione di valore, dove non è ammessa una copia. Non si può inviare una copia di denaro, si deve inviare parte del denaro[15]. In tal caso, sorge il bisogno della presenza di un terzo che sia vigile e che confermi le "risorse" di entrambe le parti di una negoziazione, e quindi l'unica soluzione è quella di affidarsi necessariamente ad un intermediario. Questi ci riporta al punto di prima, ovvero centralizzazione. Il che non deve rappresentare per forza un aspetto negativo, ma di fatto le grandi organizzazioni detengono tutte le informazioni. Di conseguenza, hanno la possibilità di gestirle o usarle a loro piacimento da un lato, mentre rappresentano un bersaglio appetibile per quei soggetti che vogliono impossessarsi di queste risorse, come ad esempio gli haker. Ma indipendentemente dalla loro volontà o vulnerabilità, la cosa certa è che le posseggono e che sono le uniche figure in grado di porre in essere, verificare e avverare, uno scambio di valore tra duo o più soggetti. Ragion per cui la loro presenza è cruciale affinché uno scambio di valore di qualsiasi genere possa avvenire, a tal punto da affidargli la logica delle transazioni in ogni

[14] Topscott D. e A., "*Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World"*, Paperback, 12 giugno 2018.

[15] In crittografia è noto come "double-spending", cioè l'uso ripetuto di uno stesso titolo valutario. Per capire meglio si consideri il seguente esempio: se un soggetto A invia x euro ad un soggetto B, è importante che dopo quei soldi non li abbia più altrimenti potrebbe rinviarli ad un altro soggetto. Quindi consiste in una truffa che permette di spendere lo stesso titolo valutario due o più volte. Nell'economia tradizionale questo problema è stato risolto dagli istituti finanziari centralizzati attraverso il proprio controllo, in modo da evitare la doppia spesa. Rappresenta invece, un potenziale problema in uno schema di cassa digitale in cui uno stesso singolo *token* digitale potrebbe essere speso più di una volta presso venditori diversi, in mancanza di un organo o di un sistema certificatore, perché un token digitale è costituito da un file che può essere duplicato o falsificato. Tratto da: Chohan, Usman W., Cryptocurrencies, 4 Agosto 2017, A Brief Thematic Review ,disponibile su SSRN: https://ssrn.com/abstract=3024330 oppure http://dx.doi.org/10.2139/ssrn.3024330.

tipo di commercio: dall'autentificazione, l'identificazione, alla compensazione, regolamento e registrazione.

In conclusione, l'obiettivo non è entrare nel mero carattere politico o filosofico del comportamento degli intermediari, piuttosto evidenziare la posizione centrale, intorno alla quale si basa un sistema economico. Senza tralasciare neanche i problemi delle sue inefficienze. Proprio così, basta pensare che se si vuole inviare un file o una mail basta il tempo di un click mentre se si vuole inviare denaro, i tempi si allungano drasticamente. Un paradosso ingiustificabile pensando alle tecnologie attuali, che se pur avanzatissime, rispondono sempre alla dinamica sopra indicata. Per non parlare dei costi che variano dal 10 al 20%, in relazione a fattori come luogo fisico, spread, tassi di cambio[16]. Insomma, quando si tratta di trasferire valore ci sono tempi e costi sono elevati, non al passo con una società veloce e dinamica come quella odierna.

"*Ma se oltre all'internet dell'informazione ci fosse l'internet del valore? Una specie di registro contabile distribuito a livello globale installato su milioni di computer, che fosse accessibile a tutti. Dove risorse di ogni tipo, dal denaro alla musica, potrebbero essere conservate, trasferite, scambiate e gestite senza il supporto di un intermediario. Se ci fosse un mezzo naturale per il valore?"*.[17] Non è un qualcosa di futuristico né tanto meno utopico, ma è il motivo per il quale si è definito Blockchain come un'innovazione rivoluzionaria.

"*Stiamo per affrontare un cambiamento radicale ancor più radicale evoluzione nel modo in cui interagiamo e commerciamo, perché per la prima volta, possiamo ridurre l'incertezza, non solo tramite le istituzioni politiche ed economiche, ma anche solo attraverso la tecnologia"*[18].

1.2.1 Definizione di Blockchain

Esistono diverse definizioni di blockchain (letteralmente "catena di blocchi), ma è possibile immaginarla semplicemente come un insieme di blocchi concatenati, che contengono l'insieme delle transazioni validate, in grado di collegare i diversi nodi, che

[16] Michkin F. S., Eakins S. G., Forestieri G., "*Istituzioni e mercati finanziari",* Pearson Italia, 1 settembre 2015.
[17] Tapscott D., "*How the blockchain is changing money and business"*, TEDSummit, giugno 2016.
[18] Warburg B., "*How the blockchain will radically transform the economy"*, TEDSummit, giugno 2016.

a sua volta sono formati dai server di ciascun partecipante [19]. In pratica è un registro pubblico, strutturato in blocchi, contenente la cronologia di tutte le transazioni avvenute dal momento zero, ossia dalla genesi dei *blocks*, sino ad oggi. Inoltre, è custodito e condiviso da tutti i partecipanti al sistema, detti nodi. Infatti, diversamente dalle architetture tradizionali *client-server*, che distinguevano nettamente il ruolo di colui che richiede la risorsa (il client) da colui che la eroga (il server), la blockchain si basa su una rete di tipo peer-to-peer. Ciò significa che adotta un approccio da pari a pari, ogni partecipante è sullo stesso livello, non ci sono distinzioni gerarchiche, in modo tale che ognuno può avere accesso in qualsiasi momento all'intero database delle transazioni, attraverso quindi una modalità trasparente e non centralizzata. Dopo una breve analisi, Mauro Bellini, direttore e responsabile di diverse testate giornalistiche, riesce ad elaborare una descrizione concisa ma esaustiva del fenomeno in oggetto: "*la Blockchain è una tecnologia che permette la creazione e gestione di un grande database distribuito per la gestione di transazioni condivisibili tra più nodi di una rete.*"[20]. Come si può evincere gli elementi principali sono i blocchi e i nodi, i primi rappresentano i contenitori dell'informazione mentre i secondi, sono costituiti fisicamente dal server attraverso il quale ogni utente ha accesso alla blockchain. Questi ultimi in particolare vedono, controllano e approvano tutte le transazioni. Tuttavia, esiste una categoria particolare di nodi, i c.d. *miners*, che utilizzano un'elevata quantità di risorse (energia elettrica e computer di ultima generazione), e quindi caratterizzati da un'elevata potenza computazionale per risolvere i problemi matematici-crittografici generati dalla rete. Dunque, la Blockchain raffigura l'evoluzione del concetto di "*ledger*", ovvero libro mastro[21] decentralizzato, in "*distributed ledger*"[22]. Pertanto, una tecnologia che non solo consente la decentralizzazione dell'informazione, la quale non è più custodita da un'unica unità centrale ma diretta invece verso le periferie. Ma in aggiunta permette, a tutti i nodi

[19] Francesca A., "*Blockchain e smart contract: funzionamento e applicazioni"*, Altalex.com, 29 aprile 2019.
[20] Bellini M., "*Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia"*, Blockchain4innovation.it, 26 settembre 2019.
[21] *"l Ledger è il "Libro Mastro", ovvero la base fondamentale della contabilità. Si può ben dire che i Ledger rappresentano una delle basi della nostra civiltà e del nostro modo di interpretare e gestire le relazioni e le transazioni tra persone e tra organizzazioni. […] fanno poi riferimento a degli* ***Archivi o Registri****. In altre parole, il Ledger ha in valore nel momento e nella misura in cui può essere consultato e permette di stabilire una memoria storica, per controllare, verificare, gestire le transazioni e gli scambi che sono stati effettuati."*. Una spiegazione più precisa fornita da Bellini M., *Che cosa sono e come funzionano le Blockchain Distributed Ledgers Technology – DLT*, blockchain4innovation.it, 27 dicembre 2018. Per maggiori informazioni consultare il seguente link: https://www.blockchain4innovation.it/esperti/cosa-funzionano-le-blockchain-distributed-ledgers-technology-dlt/.
[22] Tipologia di registro analizzata successivamente (Vedi paragrafo 1.5).

(partecipanti alla rete), la possibilità di disporre in egual modo e in qualsiasi momento delle stesse informazioni. Quindi, si può affermare che l'inedito sistema introduce, o quanto meno mira ad un nuovo concetto di governance: non più basato sulla possibilità che un soggetto possa prevalere sugli altri (in termini di potere sulle informazioni), ma invece basato sulla fiducia tra tutti i soggetti. Gli stessi che, detenendo le stesse informazioni degli altri, parteciperanno nella stessa misura al processo decisionale.

1.2.2 Il funzionamento e gli usi della *catena di blocchi*

Dunque, la Blockchain si basa su una rete di computer, ovviamente connessi ad internet, ma la cosa fondamentale è la struttura delle transazioni basate su una *crittografia robusta a "doppia chiave"*. Nello specifico, un meccanismo fondato su un'architettura tecnologica avanzata, complessa e una relazione chiave privata/ chiave pubblica. La prima chiave permette agli utenti di firmare la transazione e si associa univocamente a quella pubblica, la seconda invece verifica l'autenticità della firma e rappresenta l'indirizzo del portafoglio, chiamato address (formato dai 25 ai 36 caratteri). In sostanza, la chiave pubblica è come se fosse l'indirizzo e-mail che consente di trasferire bitcoin verso un destinatario, mentre la chiave privata (formata da 256 bit e rappresentata in 64 caratteri) è la firma del messaggio che permette di spendere i bitcoin. Definiti gli aspetti prettamente tecnici che si celano dietro un'operazione, resta da capire cosa succede quando ne avviene una. Prima ancora però c'è da dire che, il presupposto essenziale affinché sia valida una transazione, è la conferma della rete. Quindi, per essere valido uno scambio di una risorsa X da un soggetto A ad un soggetto B, c'è bisogno dell'approvazione della rete. La transazione, vista come un problema matematico, una volta effettuata, viene notificata a tutti i nodi, cosicché questi possono verificare singolarmente e indipendentemente la reale disponibilità della risorsa (crypto-asset) in capo ad A. Comunemente viene chiamato *processo di verifica indipendente*, perché si differenzia dalla successiva fase di validazione in cui entrano in gioco altri meccanismi. Nel medesimo istante, il sopracitato problema si va ad inserire all'interno di un blocco. In pratica succede che: col passare del tempo, nello specifico ogni 10 minuti, si genera un contenitore chiamato blocco, dove al suo interno ci sono tanti problemi matematici (transazioni). Tuttavia, ogni qual volta se ne genera uno, contenente tutte le transazioni precedenti avvenute, entrano in gioco i *miners*. Questi ultimi, in possesso di un'enorme

potenza computazionale, che viene messa a disposizione del sistema, competono tra di loro per risolvere i complessi problemi matematici-crittografici generati dalle numerose transazioni contenute in un blocco. A questo punto il miners/nodo validatore che trova la soluzione la comunica al network, affinché essi possano confermare o meno. Ovviamente si parla dell'operazione in base ai dati (chiave pubblica/privata) dei soggetti e delle risorse relative allo scambio. Nel caso in cui i precedenti processi descritti vadano a buon fine, il *miner* che per prima risolve il problema riceve in cambio un "premio", che sostanzialmente è un'unità di criptovaluta, mentre il blocco risolto e convalidato si va ad aggiungere a quello precedente in ordine cronologico. Una volta aggiunto, quindi registrato, diviene parte del sistema e di conseguenza non può essere cancellato o modificato (*immutabilità del registro*). In altre parole, i dati ivi presenti divengono permanenti e visibili da tutti i membri della rete. Va aggiunto che, le transazioni validate all'interno dei blocchi sono correlate da un marcatore temporale (il cosiddetto *timestamp*) e ogni blocco contiene l'*hash*[23] del blocco precedente, ovvero un valore/codice che collega i blocchi tra di loro. Il risultato è una struttura a forma di catena in cui ogni elemento addizionale verifica e rinforza quelli precedenti. È evidente che più le catene sono lunghe, più è difficile la loro manomissione. La lunghezza però non è l'unica in grado giustificare l'affidabilità e la sicurezza del sistema blockchain, anzi bisogna considerare e approfondire altri aspetti. Innanzitutto, uno di questi è rappresentato da una questione già accennata in precedenza, cioè la caratteristica di registro distribuito. Ciò infatti, permette al database di trovarsi fisicamente su più server (computer) nello stesso momento, tutti sincronizzati alla perfezione, e non solo su uno. In aggiunta, attribuisce al sistema una maggiore potenza di calcolo, in quanto può contare sulle risorse di tutti i computer connessi. Si può notare quindi, l'importanza della funzione dei nodi che risultano essere allo stesso tempo parte attiva e passiva dell'intero sistema, avendo il compito sia di generare e validare le transazioni sia di conservare la memoria delle stesse[24]. L'altra componente è la ricompensa, in criptoasset o criptovaluta in base alla piattaforma di riferimento, che il sistema riconosce al nodo che risolve il problema-crittografico. Altro non è che il pagamento per il lavoro compiuto. Lo stesso Nakamoto scrive nel suo paper che l'incentivo aiuta e incoraggia un comportamento onesto da parte

[23] "*L'hash è una funzione non iniettiva (e quindi non invertibile) che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita"* De Collibus F. M., Mauro R., "*Hacking Finance – la rivoluzione del bitcoin e della blockchain*", Milano, Agenzia X, 2016.
[24] Cataldo A., Campara F., "*Blockchain, criptovalute, smart contract, industria 4.0",* Pacini Editore, 2019.

dei nodi[25]. In definitiva, il connubio dei due elementi, ovvero la potenza computazionale della rete blockchain (c.d. *hashrate*) dovuta al registro distribuito e la complessità determinata a livello algoritmico di soluzione/generazione dei blocchi, attribuisce un elevato livello di difficoltà al problema da risolvere.

Da un'altra prospettiva invece, rendono idea di quanto basse siano le possibilità di manomissioni del finora descritto protocollo di fiducia. Infatti, si stima che la possibilità di violazione della blockchain è uguale a una sull'intero numero di atomi dell'universo[26]. A dire il vero esiste, seppur con bassissima probabilità, un modo per farlo: c'è bisogno che un solo nodo sia in possesso di risorse maggiori di quelle dell'intera rete messa insieme. "Basterebbe" anche che riuscisse ad avere una potenza tale da raggiungere il 50% più uno dell'intera capacità di calcolo del network per modificare un blocco, soltanto che la modifica risulta un'operazione ardua o quasi surreale, poiché l'intervento di modifica deve essere diretto nei confronti di tutti i blocchi successivi fino ad arrivare a quello che si intende manomettere. Si può capire che risulta al quanto impossibile, se si considera in aggiunta che con il meccanismo delle ricompense proprio della blockchain e basato sulla teoria dei giochi, è più conveniente mettere a disposizione della rete le proprie risorse per guadagnare monete (*fare mining*) piuttosto che sovvertirlo. Infatti, ammesso e concesso che per assurdo si verifichino tali condizioni, e quindi che il malintenzionato riesca a farlo, in realtà sta mettendo a rischio il guadagno indebitamente acquisito. In merito al fatto che, se il soggetto facesse questa operazione più di una volta, comprometterebbe la fiducia del sistema, rendendo così vano l'utilizzo degli asset rubati.

Alcuni ritengono che la blockchain assuma le vesti di una nuova *forma mentis*, un nuovo approccio che per certi versi può essere definito politico, dato luogo da una piattaforma capace di sviluppare e concretizzare una nuova forma di democrazia. Realtà distribuita capace di assicurare a tutti i suoi utenti la facoltà di disporre, controllare e verificare la trasparenza degli atti e delle decisioni, a sua volta contenuti in registri condivisi con la peculiarità di essere immutabili, immodificabili e inalterabili[27]. Prima di affrontare le varie configurazioni è fondamentale chiarire l'uso del termine riferito alla tecnologia.

Infatti, quando si usa la parola "Blockchain", con l'iniziale maiuscola, si intende l'originale registro distribuito e condiviso di Bitcoin, dove tra i due intercorre un rapporto

[25] Satoshi Nakatomo, *Bitcoin: A peer-to-Peer Electronic Cash System,* 2008

[26] De Collibus F. M., Mauro R., "*Hacking Finance – la rivoluzione del bitcoin e della blockchain*", Milano, Agenzia X, 2016.

[27] Cataldo A., Campara F., "*Blockchain, criptovalute, smart contract, industria 4.0",* Pacini Editore, 2019.

rispettivamente di tecnologia e risorsa. La stessa parola blockchain, usata invece con la minuscola, si intende l'architettura tecnologica c.d. *distribuited ledger* (vedi nota 21) che usa criptoasset diversi dal bitcoin. In particolare, blockchain è una sottocategoria del DLT (*distribuited ledger technology*) ciò significa che non tutte le tecnologie basate su registri distribuiti e condivisi hanno una struttura a catena di blocchi[28]. Pertanto, alla luce di quanto detto, è possibile affermare ai fini di una comprensione corretta del fenomeno, che esistono diverse tipologie di blockchain sia in base al tipo di registro DLT utilizzato e sia in base alle svariate criptovalute impiegate come strumento, ad esempio bitcoin, ethereum, litecoin.

1.2.3 Una rassegna delle diverse tipologie di *blockchain*

Fino ad ora si è preso un unico modello in considerazione, la c.d. blockchain pubblica o *permissionless*, lo stesso che si terrà in considerazione anche in seguito in ambito di analisi. Ma è doveroso distinguere le varie tipologie in base all'impostazione del registro così da poter, nei prossimi capitoli, esporre al meglio le diverse fattispecie normative a riguardo. Infatti, il quadro normativo disciplina in maniera univoca le criptovalute, ma non i registri, quindi non avrebbe senso aprire una parentesi approfondita sulle prime, piuttosto si provvederà semplicemente nell'individuare quali siano a differenza del secondo caso. Sostanzialmente le principali tipologie di blockchain in base ai registri ne sono tre: pubbliche (*permissionless*), private (*permissioned*) e ibride (*hybrid*). Per quanto riguarda la prima, già descritta, può essere riassunta nei seguenti punti:

- è ad accesso libero, chiunque tendenzialmente può parteciparvi;
- non esiste alcun proprietario né tanto meno un intermediario di riferimento che controlla o valida, ovvero "*trusted*". Il concetto di base con cui è stata concepita è l'assenza di forme di controllo;
- è prevista un'identificazione dei partecipanti attraverso uno pseudo-nome;
- non ha restrizioni di qualsiasi genere sull'attuazione e la conoscenza delle transazioni, una volta raggiunto il consenso. Di conseguenza nessun nodo, a prescindere delle risorse a disposizione, può interferire con il normale svolgimento;

[28] Cataldo A., Campara F., "*Blockchain, criptovalute, smart contract, industria 4.0",* Pacini Editore, 2019.

- perfettamente compatibile per database contenenti documenti che necessitano di essere invariati nel tempo, a meno di aggiornamenti che richiedono la massima sicurezza in termini di consenso, come ad esempio i contratti di proprietà o i testamenti;
- caratterizzata da un protocollo di consenso distribuito basato sulla *Proof of Work*[29] (PoW) o *Proof of Stake*[30] (PoS) tipiche di Bitcoin o Ethereum.

Altra categoria invece è rappresentata dalle *permissioned blockchain*, o più comunemente c.d. private, che possono essere riassunte nei seguenti punti:

- Sono ad accesso condizionato, il che vuol dire che c'è bisogno di avere determinati requisiti o essere autorizzati.
- Al loro interno ci sono uno o più intermediari (*trusted*) che controllano l'accesso e gestiscono il funzionamento, di conseguenza l'aggiunta di dati non è soggetta ad approvazione della maggioranza degli utenti e l'intero sistema può essere di loro proprietà.
- Tutti i nodi, utenti e miners, possono essere identificati in maniera chiara. Cioè si può risalire ai soggetti in capo ad essi.

[29] PoW tradotta letteralmente significa prova di lavoro, ciò che l'algoritmo di questa blockchain richiede ai *miners*. I quali nel fare mining, ovvero per ottenere monete/premi per la risoluzione di problemi crittografici, si ritrovano a dover svolgere un task molto dispendioso in termini di tempo ed energia. In questo modo il protocollo rende estremamente svantaggioso, da un punto di vista economico, tentare di riscrivere o compromettere la catena di blocchi. Proprio perché, più una transazione si trova in profondità nel registro maggiore sarà il lavoro che un nodo deve affrontare per poterla modificare o eliminare e ricostruire tutti i blocchi successiva ad essa, mentre altri blocchi continuano ad aggiungersi aumentando la catena grazie al lavoro di altri utenti. Vedi Valsecchi V., *La classificazione delle Blockchain: pubbliche, autorizzate e private*, in Spindox.it, 20 giugno 2018 (https://www.spindox.it/it/blog/la-classificazione-delle-blockchain/#).

[30] PoS può essere tradotta in italiano come "prova che si ha un interesse in gioco", in questo modello *il numero di token di valuta digitale detenuti da ciascun utente, è una questione importante all'interno del sistema. Più grande è la partecipazione ("stake"), ovvero la quantità di token posseduti da un utente, maggiori sono le probabilità che non si stia violando il sistema. Ancora, più un individuo è esposto ad una criptovaluta, più è probabile che questi si comporti in modo ottimale.[…] I partecipanti che possiedono una partecipazione significativa nei sistemi Proof of Stake vengono selezionati su base pseudocasuale per coniare i blocchi e aggiungerli alla blockchain. Il processo di selezione pseudocasuale entra in funzione dopo che il sistema ha analizzato diversi fattori al fine di garantire che siano selezionati solo gli individui con una quota maggiore, ma anche altri con una stake inferiore. IL Proof of Stake viene applicata generalmente alle criptovalute pre-minate, così da consentire all'utente di accedervi attraverso la partecipazione. Ciò significa che l'offerta complessiva delle criptovalute Proof of Stake viene fissata sin dall'inizio e che non vi è alcun premio per la creazione dei blocchi, come avviene invece nella Proof of Work. L'unico incentivo per i miners in questo sistema è rappresentato dalle commissioni di transazione associate allo specifico blocco coniato.* Vedi Provenzani F**.,** *Cos'è il Proof Of Work (PoW) e Proof Of Stake (PoS)*, Money.it, 29 aprile 2019 (https://www.money.it/Cos-e-la-Proof-Of-Work-PoW-e-Proof-of-Stake).

- Possono essere più performante e veloci di quelle pubbliche da un punto di vista tecnico.
- Sono ideali per grandi intermediari, come istituzioni, banche o imprese che devono gestire filiere con una serie di attori, perché gli consente la possibilità di controllo sulle modalità di esecuzione delle transazioni. In altre parole, gli garantisce maggiore trasparenza e sicurezza sull'operato degli utenti autorizzati.

Esiste, infine, un'ultima categoria chiamata *hybrid blockchain*, le c.d. hibride, che sono caratterizzate dal fatto di possedere elementi di entrambe le classi precedenti. In sintesi quindi:

- Possono essere ad accesso condizionato o meno.
- I nodi non sono sullo stesso piano, in termini di operazioni eseguibili, infatti vengono chiamati *contributor* anziché *peer*.
- Sono parzialmente decentrate, dato che pochi utenti (conosciuti e preselezionati da un "terzo") hanno un peso maggiore all'interno della rete, potendo quindi gestire e validare il consenso. Più precisamente, sono loro a decidere quali transazioni inserire in un blocco.

1.2.4 Token: il cardine di un sistema transazionale

Per dare una visione chiara e completa del fenomeno blockchain, affrontato in quasi tutte le sue sfaccettature, bisogna introdurre un altro concetto chiave: i token. In precedenza, sono state affrontate tutte le questioni tecniche e funzionali riguardanti la tecnologia, ora invece si avrà modo di qualificare i mezzi sulla quale si basa, che quindi divengono essenziali per qualsiasi tipo di transazione all'interno della rete. Un token, infatti, è un asset digitale che può essere scambiato tra due parti senza l'intervento di un ente terzo o intermediario. Può essere identificato come un'informazione digitale (o un set di informazioni) capace di conferire ad un soggetto una serie di diritti, alcuni dei quali governati da un sistema di smart contracts, soprattutto quello di proprietà sulla medesima. Quest'informazione viene registrata in un blocco della catena è può essere trasferita mediante un protocollo. Riassumendo e adottando una corretta definizione, il token è un asset digitale che è oggetto di scambio all'interno di una piattaforma DLT. Di conseguenza, rappresenta il fulcro di un sistema transazionale, in cui la validità dei negozi

giuridici sottostanti è assicurata da un sistema matematico in grado di ricreare un rapporto fiduciario anche tra soggetti che non si conoscono reciprocamente, senza che sia necessaria l'azione di un'entità terza intermediaria[31].

L'elemento principale risulta quindi la capacità di conferire una svariata quantità di diritti al soggetto che li detiene. Infatti, in base sia dal tipo di approccio tecnologico e sia dal tipo di utilizzo, esistono diverse tipologie di token divise in tre macro-aree[32]:

- i token di classe 1, ovvero tutti quelli che hanno la funzione di registrare un diritto di proprietà del token stesso al soggetto che li detiene e quindi una tipologia che non conferisce diritti nei confronti di una controparte. Un vero e proprio *coin* che può essere trasferito tramite una transazione su blockchain. Quindi, in poche parole con questa tipologia di token il proprietario ha il solo diritto di proprietà sullo stesso. Di questa categoria fanno parte i token di criptovalute come Bitcoin, Litecoin, Bitcoin Cash.
- I Token di classe 2, i quali assegnano ai proprietari una serie di diritti che possono essere esercitati nei confronti di terzi o nei confronti del soggetto (o soggetti) che ha generato il token. A differenza della prima classe, questi permettono al suo possessore di esercitare diritti verso le controparti. È possibile fare una comparazione con il codice civile italiano, configurandoli come una sorta di titoli di credito come *titoli obbligazionari, titoli di partecipazioni, titoli rappresentativi di merci e documenti di legittimazione, titoli di prestito*. Infatti, secondo l'art.1992 c.c. questi documenti conferiscono al possessore il "*diritto alla prestazione in esso indicata verso presentazione del titolo*". Rientrano in questa categoria token per smart contract relativi alla gestione dei pagamenti futuri, token come asset, token utilizzati per pagamenti standardizzati, token per la gestione di presentazione di servizi.
- Infine, ci sono i token di classe 3, cioè quelli che hanno una funzione ibrida o mista. Quindi, sono token che conferiscono sia il diritto di proprietà e sia diritti diversi.

[31] Garavaglia R., "*Tutto su Blockchain. Capire la tecnologia e le nuove opportunità"*, Milano, 2018.
[32] Bellini M., "*Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia"*, Blockchain4innovation.it, 26 settembre 2019.

1.2.5 I processi evolutivi delle *Initial Coin Offering*

Ulteriore caratteristica della blockchain è la capacità di raccolta di capitali ai fini imprenditoriali, che può avvenire attraverso appunto la piattaforma. Tale modalità viene chiamata ICO (ovvero *Initial Coin Offering*) e consente a soggetti, che vogliono intraprendere un progetto imprenditoriale, di ottenere capitali attraverso questa forma digitale basata esclusivamente su registri distribuiti. Diversi sono i motivi per i quali le ICO hanno ricevuto una così grande diffusione e quindi successo, ma sostanzialmente possono essere riassunti in due fattori: innanzitutto tali iniziative non erano in alcun modo regolamentate e, in secondo luogo, il loro processo di avvio risultava alquanto semplice. Nello specifico il processo attraverso il quale avviene la suddetta raccolta è strutturato da tre fasi[33]. La prima si basa sulla redazione e pubblicazione di un particolare documento chiamato *whitepaper* (libro bianco), da parte del soggetto richiedente. Al suo interno vengono descritte e stabilite una serie di informazioni, come la descrizione del progetto imprenditoriale, la funzione assunta dal token all'interno del contesto progettuale e la modalità di distribuzione dei token sul mercato. La fase successiva è costituita dalla raccolta di capitale, che avviene mediante la compravendita di token di nuova emissione con l'unità di criptovaluta di riferimento, che rappresenta quindi il prezzo da pagare per ottenere il token in questione. Sono i promotori dell'ICO a fissare i requisiti tempistici o di capitali da raggiungere in questa sezione. Infine, al termine del secondo step, il nuovo token viene immesso all'interno di una piattaforma di scambio, chiamata *exchange*, in modo da consentire la sua negoziazione. Una volta completato il ciclo, che vede come conclusione l'ottenimento della somma di capitale richiesta da parte del promotore, quest'ultimo può ed è tenuto ad avviare la realizzazione del progetto dichiarato all'interno del *whitepaper*. Detto questo, c'è la possibilità di dare un'immagine più comprensibile sia della figura dei token che delle ICO e sia del legame che intercorre tra le due. Infatti, si riporta integralmente un esempio fatto da Mauro Bellini all'interno di uno dei suoi articoli: "*Per capire cosa sono i token e come funzionano si può utilizzare l'esempio dei gettoni della SIP (la "vecchia" compagnia telefonica del passato). I gettoni telefonici servivano per ottenere un servizio molto concreto: la telefonata dalle cabine pubbliche. Il gettone era un token e aveva un valore di 50 lire. Una ICO è, per certi aspetti, si emette un token che serve per usufruire di un servizio. In questo modo la società ottiene delle risorse che può utilizzare senza contrarre nessun obbligo nei confronti di chi ha effettuato*

[33] Cataldo A., Campara F., "*Blockchain, criptovalute, smart contract, industria 4.0",* Pacini Editore, 2019.

gli investimenti (differentemente dagli IPO, dove gli obblighi naturalmente ci sono) se non quello di rendere poi disponibile il servizio a chi sarà pronto a pagarlo con il proprio token, ovvero spendendo l'asset di valore che ha acquistato in fase di ICO. Il vecchio gettone della SIP come il token può essere scambiato in ragione del suo valore intrinseco. Un gettone SIP aveva un valore riconosciuto di 50 Lire che i negozianti accettavano perché avevano la certezza di rimettere in circolazione quella "moneta" che di fatto era un asset di valore. Dunque, il gettone nato per l'erogazione di un servizio (la telefonata dalle cabine pubbliche) era diventato un asset utilizzato anche per la gestione di piccole transazioni. Se la società titolare del servizio e protagonista dell'emissione decideva, legittimamente, che il valore della telefonata non era più assimilabile a un gettone di 50 Lire bensì a un valore di 100 Lire e conseguentemente "aumentava" il valore del gettone ecco che chi aveva acquistato un certo numero di gettoni (non per un investimento ma in previsione di fare molte telefonate) si trovava ad avere lo stesso valore in termini di "quantità di servizi telefonici" ma un valore raddoppiato in termini di "asset di valore" da utilizzare "sul mercato" come "moneta" di scambio. Il token delle ICO è un po' come il gettone della SIP. Se chi lo emette promette di erogare un servizio che può essere acquistato grazie al token, si ritrova con un investimento fatto da soggetti che intendono utilizzare quel servizio o che credono nel valore di quel servizio al punto da acquisire tanti "gettoni" per utilizzarlo o per "venderli" ad altri che potranno utilizzarli. Se dietro al token non ci sono servizi il rischio è che si tratti solo di una nuova forma di investimento. Ecco che appare molto importante analizzare con attenzione tutte le varie forme di token"[34].

Illustrato il concetto, non si può negare che le ICO sono state oggetto di discussione negli ultimi anni, data la loro natura. Infatti, spesso sono state utilizzate come strumento per mettere in atto speculazioni finanziarie o, addirittura, in tanti altri casi non esisteva alcun progetto industriale alla base o quantomeno non era all'altezza delle aspettative. Ma, come sempre nella storia, ogni qual volta si presentano delle criticità senza apparente soluzione, nascono nuovi strumenti per risolvere l'arcano. A tal proposito, sono nate le STO, ovvero *Security Token Offering* che possono rappresentare un'evoluzione delle ICO. Si basano sullo stesso principio, cioè la possibilità di ricevere capitali necessari attraverso l'emissione di token su una piattaforma blockchain per realizzare un'idea di business, ma con una differenza sostanziale: i *security token* possono essere oggetto di

[34] Bellini M., "*Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia"*, Blockchain4innovation.it, 26 settembre 2019.

trading. Il che significa, che gli stessi devono essere assicurati e basati su un bene tangibile, misurabile e concreto.[35] In questo modo il bene può essere scambiato con un token, cosicché quest'ultimo possa, a tutti gli effetti, rappresentarlo anche nel mondo reale.[36] A differenza di quanto succedeva con le ICO, nate con l'obiettivo di finanziare lo sviluppo di idee di business rivelandosi pertanto uno strumento simile al *crowfunding*[37], ma nella pratica diventate uno strumento per l'emissione di token come asset di scambio, soggetti quindi a speculazione o ad altri fini, e non come asset generato come esclusiva forma di investimento. Il risultato è che le STO si configurano come un mezzo capace di garantire maggiore sicurezza e controllo agli investitori, essendo meno soggette a frodi. In aggiunta i token su cui si basa, i security token, rappresentano a tutti gli effetti una forma di investimento, assumendo la caratteristica di un asset vero e proprio che offre perciò una serie di vantaggi, come ad esempio i diritti di tipo finanziario. D'altro canto, in quanto tali però, sono soggetti a una regolamentazione. Riassumendo, si può affermare che "*i security token sono la rappresentazione, sulla blockchain, di strumenti finanziari tradizionali come azioni o obbligazioni, sono strumenti soggetti alla regolamentazione finanziaria esistente e prevedono forme di controllo e di sicurezza per gli investitori"*[38].

Altro aspetto interessante della vicenda è che con l'avvento del crowfunding e delle ICO si segna una svolta nel mondo del Venturing, legato a logiche di valutazione da parte di banche e o fondi di investimenti. In altre parole, mentre prima le start up dovevano superare rigide regole di processi di valutazione per ottenere dei finanziamenti da parte di investitori istituzionali e non, oggi possono ottenere risorse in modo più flessibile: semplicemente attraverso la blockchain, dove le start up riescono ad ottenere i capitali necessari tramite l'erogazione di token.

---

[35] Bellini M., "*Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia"*, Blockchain4innovation.it, 26 settembre 2019

[36] Ibidem.

[37] Il termine è l'incrocio di due parole, crow e founding, che tradotte singolarmente significano folla e finanziamento. Si riferisce infatti, ad uno strumento volto alla ricerca di finanziamento tra la folla. Più precisamente, si parla di piattaforme che si avvalgono del web e che permettono, per lo più a start-up, di raccogliere i fondi necessari per lo sviluppo dell'idea. Tutto ciò avviene a fronte della cessione di parte dell'equity, ma con il vantaggio di potersi rivolgere ad una platea sostanzialmente illimitata, che cede liberamente quota delle proprie risorse economiche.

[38] Bellini M., "*Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia"*, Blockchain4innovation.it, 26 settembre 2019.

Da quanto detto, risulterebbe naturale trovare delle somiglianze con quella che nell'economia reale viene chiamata IPO[39](Initial Coin Offering). In effetti, il fine è lo stesso: sono strumenti disegnati per conferire un "consenso monetario"[40] nei confronti di un'idea o di un business da parte di una comunità. In aggiunta, i token possono essere soggetti a scambio o ad oscillazioni di valore in base a fattori come l'andamento del progetto presentato o del sottostante (valore delle criptovalute alla base), assumendo a tutti gli effetti lo stesso ruolo delle azioni per un'impresa quotata. Tuttavia, c'è una sostanziale differenza, dato che quando si parla di comunità non si intende un mercato regolamentato, bensì una platea operante su blockchain. Di fatto, nel caso delle IPO, tutte le operazioni sono soggette a controllo da parte di un organo di vigilanza, che nel caso dell'ordinamento italiano è rappresentato dalla Consob, la quale ha il ruolo si sorvegliare sulla correttezza delle procedure di acquisto e di vendita di tutti gli operatori. Nelle ICO invece, in ragione del principio di decentralizzazione proprio della blockchain, non esiste, almeno fino ad ora, alcun ente che svolga tale funzione.

1.2.6 L'ambito di applicazione e i punti di forza

L'ultima questione da affrontare è l'ambito di applicazione, senza tralasciare in che modo la blockchain può cambiare, migliorare determinati settori anche molto differenti tra di loro. Non a caso, uno dei motivi dell'enorme successo riscosso a livello globale, deriva proprio dalla sua versatilità d'impiego. Prima però, è doveroso fare un breve accenno ai suoi punti di forza, chiarendo e sintetizzando argomenti trattati in precedenza, così da avere uno schema completo e conciso. Solo procedendo in questo modo si potrà avere una migliore chiave di lettura. I punti su cui si basa sono sostanzialmente i seguenti:

- Peer to peer (P2P) alla base del potere distribuito. Controllo, gestione e governo diretto del sistema da parte di tutti, nessun nodo escluso, i suoi componenti. Escludendo la possibilità di concentrazione del potere decisionale in mano ad una o più entità centrali.

[39] Strumento che permette ad una società di collocare equity nel mercato principale a fronte di finanziamenti. Per un maggior grado di dettaglio, si rinvia al seguente link: https://www.borsaitaliana.it/borsa/glossario/ipo-offerta-pubblica-iniziale.html.
[40] Si intende il riconoscimento di valore nei confronti di una società che consente il successivo apporto di capitali da parte di un operatore di mercato.

- Meccanismo di consenso, che attribuisce un elevato grado di sicurezza e affidabilità alla catena e mette in risalto il ruolo centrale del network.
- Trasparenza, tracciabilità e solidità di tutte le operazioni eseguite sulla blockchain. Infatti, qualsiasi utente ha la possibilità di prendere visione di ogni transazione già registrata o in corso di validazione, le quali sono sorrette da una crittografia robusta che le rende immodificabili e irrevocabili. In questo modo, l'intero sistema risulta più solido e attendibile.
- Privacy maggiore degli utenti che, attraverso meccanismi di pseudonimizzazione, hanno la possibilità di non mostrare dati personali o credenziali a loro riconducibili.
- Valore come incentivo che rappresenta un principio cardine tramite il quale ogni nodo, sotto varie forme, è spinto a contribuire al funzionamento del sistema. Partecipanti che concorrono ad alimentare la potenza computazionale di una piattaforma mettendo a disposizione le loro risorse (computer), a fronte di vari benefici: i *miners* incentivati da logiche di remunerazione e insieme agli altri nodi da logiche di velocità, affidabilità, sicurezza, trasparenza ed economicità.

I contesti in cui queste caratteristiche potrebbero fare la differenza sono abbastanza numerosi ed eterogenei tra di loro. Tuttavia, in alcuni la blockchain ha già assunto una posizione di rilievo, mentre in altri rappresenta ancora una potenziale ma non remota applicazione. Il primo che potrebbe saltare all'occhio è a) il settore economico e finanziario, che per ragioni sia storiche che prettamente applicative, rappresenta una delle principali aree di investimento in blockchain. Basta pensare all'assenza di intermediari, banche o istituti, per comprendere i vantaggi in termini di costi di commissioni sulle transazioni da un lato e l'affidabilità/velocità dall'altro. Si provi a pensare ai costi e alle tempistiche di pagamenti digitali in ambito nazionale e non, a tutte le funzioni di *backoffice* o di gestione. In altre parole, diviene uno strumento incentrato su una gestione efficace ed efficiente che comporta un ingente risparmio per l'intero sistema, in contrapposizione ad uno ormai obsoleto. Stesso discorso vale anche per b) il settore assicurativo, poiché in aggiunta, attraverso l'implemento di questa tecnologia, permette la formazione di una migliore *governance*, sicura e decentralizzata, capace di prevenire frodi, in ragione della possibilità di disporre di informazioni e report più accurati e attendibili. Altro settore in cui la blockchain può esprimersi al meglio è tutto l'ambito della c) *supply chain*, divenuto ormai un aspetto sempre più cruciale all'interno di tutta

l'industria della trasformazione tanto in termini di tracciabilità e trasparenza della catena di approvvigionamento, quanto dell'intera filiera produttiva[41]. Elementi di particolare attenzione non solo per le aziende, ma anche per il consumatore finale, che risultano essere sempre più attenti alla qualità, provenienza e originalità dei prodotti. Nella pratica, si realizza attraverso un'infrastruttura che permetta di fornire, ma soprattutto condividere in tempo reale tutta una serie di informazioni circa merci e prodotti, ma anche container e trasporti. Un vantaggio da un punto di vista di tracciabilità e certificazione, difatti, entrambe verranno consolidate da un registro in cui ogni attore (dal produttore di materia prima al consumatore finale) ha la possibilità di conferire ad ogni *step* informazioni e allo stesso tempo controllare con la massima trasparenza quelle degli altri. Settori come l'agrifood o la moda risultano, concretamente, i possibili e i principali candidati a giovare dei benefici che la blockchain può apportare. Benefici che si traducono in valore sia per l'intero settore che per l'ecosistema, rafforzando i *brand* attraverso la valorizzazione della loro filiera da un lato, e generando una tendenza in grado dare risposte veritiere ad un consumatore sempre più attento dall'altro. Non è un caso se negli ultimi anni un numero sempre crescente di aziende converge verso questa direzione, capace di garantire efficienza, tracciabilità e trasparenza attraverso l'implementazione di questo nuovo strumento tecnologico.

Medesima modalità di gestione dei dati fornita dalla blockchain può essere estesa a settori come la d) sanità e la e) pubblica amministrazione, risultando una soluzione concreta e ideale ai numerosi problemi che li affliggono. Nel primo caso, basta pensare a inefficienze che coinvolgono tanto ospedali e altre strutture quanto il contribuente dovute a:

- asimmetria, accesso lento e poco sicuro alle informazioni tra i vari attori;
- sistemi gestionali molto differenti e spesso non compatibili;
- *compilance* normativa[42], in termini di gestione iterazione di sistemi sanitari disposti su veri livelli (nazionale, regionale e locale) e di diversa natura (pubblica e privata).

Ragion per cui avere un'unica piattaforma condivisa, a cui tutti possono avere accesso e capace di mettere a disposizione informazioni certe e certificate in modo tempestivo, può

[41] Bellini M., "*Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia"*, Blockchain4innovation.it, 26 settembre 2019.
[42] Cataldo A., Campara F., "*Blockchain, criptovalute, smart contract, industria 4.0"*, Pacini Editore, 2019, P. 30.

essere una soluzione non solo per quelle problematiche di coordinamento tra strutture, ma anche quelle riguardanti il paziente. In sostanza, l'adozione di blockchain può porre il settore nel suo complesso in condizioni di poter offrire un servizio sempre più di qualità, che si traduce in somministrazione di cure migliori per i pazienti, più adatte e in tempi più rapidi. Analogo discorso vale anche per la pubblica amministrazione, che può trarre benefici da un punto di vista operativo e gestionale, ma anche per quanto riguarda costi di transazione. Vantaggi che posso riguardare registri catastali e immobiliari, gare d'appalto, ma anche l'operato di operatori o pubblici ufficiali. Si configura, di fatto, oltre che una soluzione capace di rendere i processi più veloci, sicuri e meno dispendiosi, ma anche capace di fornire ottimi strumenti per la lotta contro l'evasione e la criminalità. f) Il settore energetico può essere un ulteriore ambito di applicazione della blockchain, intervenendo sulla riduzione dei costi e degli sprechi in termini di energia, attraverso una piattaforma di analisi e condivisione dei dati capace di gestire sia la produzione che i consumi. Campo diverso, ma di valida e potenziale applicazione può essere quello dei g) brevetti e proprietà intellettuale. La blockchain, in questo caso, può contribuire in primis per quanto riguarda la registrazione, e quindi da un punto di vista di infrastruttura, ma anche come mezzo per accertare la provenienza e l'originalità dei beni e asset acquisiti. Fino ad arrivare a risolvere problemi come corretta remunerazione degli attori della filiera (produttore, autore, distributore) e la diffusione e lo scambio.

1.3 Valute virtuali: difficoltà nella comprensione e nella definizione del fenomeno

Descritte le caratteristiche e le varie configurazioni della tecnologia blockchain, ora tocca spostare il focus verso le risorse utilizzate, ovvero sugli *asset* necessari, utilizzati per fare delle transazioni. Per essere più chiari, una volta definita l'architettura della tecnologia è necessario comprendere quali sono e in che modo le risorse alla base, chiamate criptoasset/criptovalute/asset, permettono il suo funzionamento.

Le valute virtuali sono in circolazione da oltre un decennio. Esse, dunque, sono 'emesse' in due forme: mediante l'opera dei 'minatori' – cripto valute - o tramite la sottoscrizione delle 'Offerte Iniziali di Moneta' (ICO - Initial Coin Offers) – gettoni o 'token'.
Nel primo caso si tratta di uno scambio delle valute virtuali 'ordinarie' (bitcoin, Ethereum, Stellar, e così via.). Per poter validare tale scambio di moneta, infatti, è necessario che

esso sia riconosciuto da tutti i nodi precedenti della catena dei blocchi (blockchain) e, affinché ciò avvenga, è indispensabile che il blocco sia 'minato'. Quando ciò avviene al 'minatore' sono assegnati una certa quantità di criptovalute. Nel secondo caso (quello delle ICO), invece, si assiste ad una forma di OPA (Offerte di Pubblico Acquisto), i cui fondi, eventualmente raccolti, non sono destinati ad aumentare il capitale di una società, ma a finanziare una start-up. In tale ipotesi, il sottoscrittore riceve, in cambio al suo finanziamento, un gettone (token) che può, poi, essere liberamente trasferito.

Le valute virtuali (criptovalute e token) hanno elementi simili a quelli delle monete correnti e degli strumenti finanziari.

Tuttavia, però, non sono assimilabili né alle prime né ai secondi. Sia l'Unione Europea sia l'Italia stanno cominciando a occuparsene anche legislativamente e si registrano i primi interventi giurisprudenziali. Le incertezze sono ancora numerose e ciò genera difficoltà nella comprensione e nella definizione del fenomeno.

All’inizio, queste valute erano state concepite quali monete alternative a quelle correnti. Si voleva, in sostanza, creare un sistema monetario elettronico indipendente da un'autorità centrale, la quale sarebbe sostituita dalla tecnologia dei registri distribuiti e condivisi, che assicurano, essendo immodificabili, l'unicità della transazione. Tale funzione è confermata dal fatto che, sia in ambito privato sia in quello pubblico, le criptovalute possono essere utilizzate, al momento, molto limitatamente, come forme di pagamento. Ci si può, quindi, chiedere se le valute virtuali possono essere paragonate a delle monete correnti o a degli strumenti finanziari.

Per quanto concerne questo secondo aspetto, si deve sottolineare che esse non sono state riconosciute come strumenti finanziari puri, poiché, attraverso questi ultimi non si possono acquistare beni e servizi (come avviene con le valute virtuali), ma solo altra moneta. Relativamente al primo aspetto, invece, la risposta all'interrogativo può essere elaborata considerando le attuali teorie economiche sul concetto di moneta e proseguendo con l'analisi delle discipline giuridiche, con particolare attenzione agli aspetti civilistici, contabili e tributari.

Le teorie economiche attribuiscono alla moneta tre funzioni: quella di riserva di valore, che consiste nella possibilità di accumulo e mantenimento del valore della moneta stessa; quella di unità di conto, ossia la possibilità di utilizzare la moneta come 'misuratore' del valore di tutte le cose che possono essere oggetto di scambio; quella, appunto, di mezzo di scambio, ossia il riconoscimento della stessa nella comunità.

In riferimento alle criptovalute è proprio quest'ultima funzione (ma c'è incertezza anche sulle altre) quella che non si realizza completamente, poiché la loro accettazione in cambio dell'erogazione di un servizio o di un trasferimento di un bene è riconosciuta da una ristretta cerchia di persone (soprattutto perché il loro valore rispetto alla valuta corrente non è stabile).

Da una visione economica, pertanto, le valute virtuali non sono assimilabili a moneta corrente[43].

In ottica giuridica, la situazione è forse più complessa e frammentata. Se da una parte le criptovalute non possono essere assimilate a un bene immateriale, perché non atte a produrre utilità pluriennale, dall'altra, nella sentenza *"Skatteverker*", relativa alla causa C-264/14, del 22 ottobre 2015, la Corte di Giustizia europea ha escluso che il bitcoin possa essere qualificato come bene materiale ai sensi della direttiva IVA. Nello stesso tempo però, ai fini della medesima direttiva, il cambio tra bitcoin, a cui si riconosce la funzione di mezzo di pagamento, e valuta corrente è categorizzato quale operazione finanziaria (quindi esente ai fini IVA).

Poco tempo dopo il Parlamento europeo, con la Risoluzione del 26 maggio 2016, aderendo a quanto espresso dalla BCE, ha affermato che una definizione di valute virtuali potrebbe essere: "*rappresentazioni di valori digitali che non sono emesse né da una banca centrale o da un ente pubblico né sono necessariamente legate a una valuta a corso legale, ma sono accettate da persone giuridiche e fisiche come mezzo di pagamento e possono essere trasferite, archiviate o scambiate elettronicamente*".

Tale definizione è presente anche nell'ordinamento italiano, precisamente nell'art. 1, comma 2, let. qq), D. Lgs. n. 231/2007 sull'antiriciclaggio, come modificato dal D. Lgs. n. 90/2017, in anticipo su quanto stabilito a livello europeo nella Direttiva n. 2018/843, da adottare entro il 2020.

Ad ogni modo, la Corte di Appello di Brescia, nel Decreto n. 207/2018, ha affermato che la valuta virtuale non ha le caratteristiche per poter soddisfare la funzione di unità di conto o di riserva di valore. Ne consegue, pertanto, che essa non può essere assimilata a una moneta. Ciò figurerebbe in linea con quanto asserito dal Tribunale di Verona, con la Sentenza n. 195/2017, che ha qualificato il bitcoin quale *"strumento finanziario utilizzato per compiere una serie di particolari forme di transazioni on line"* costituito da *"una moneta che può essere coniata da qualunque utente"*.

[43] Da Banca Centrale Europea, "*Virtual Currency Schemes"*, febbraio 2015.

Ma, al di là di questi primi interventi giurisprudenziali, anche qualora si volesse loro riconoscere la funzione di mezzo di scambio, le criptovalute, in Italia, non potrebbero essere assimilate alla moneta legale, ma sarebbero comunque riconosciute. Si richiama in proposito che l'art. 1277 del c.c., infatti, stabilisce che le obbligazioni pecuniarie possono essere soddisfatte solo mediante "*moneta avente corso legale"*. Nello stesso tempo, però, l'esistenza di monete non avente corso legale è già prevista[44]. Nell'art. 1278 c.c. è stabilito che *"se la somma dovuta è determinata in una moneta non avente corso legale nello Stato, il debitore ha facoltà di pagare in moneta legale, al corso del cambio nel giorno della scadenza e nel luogo stabilito per il pagamento"*. In sostanza, attualmente, qualunque sia il percorso interpretativo adottato, le valute virtuali non possono essere assimilate alle valute correnti (nemmeno elettroniche: Direttiva 2009/110/CE; TUB, art. 114-bis).

Le difficoltà e le confusioni indicate (la valuta virtuale non è una moneta e non è uno strumento finanziario, ma, forse, è un mezzo di pagamento) si riverberano anche in campo contabile: la valuta virtuale, che per esempio sia utilizzata per la costituzione di una società (casi avvenuti, ma che si è cercato di arginare), non può essere considerata una valuta corrente per rispetto del principio generale di prudenza, così come non può essere assimilata a un bene (materiale o immateriale). Quindi, potrebbe essere considerato un credito, ma non è certo, perché incerta ne è l'esigibilità.

La difficile definizione di 'valute virtuali' è, inoltre, aggravata, da quanto espresso, sebbene non esplicitamente, dall'Amministrazione finanziaria italiana che, formalmente, equipara la valuta virtuale alla valuta estera[45], e i gettoni (token) ai derivati[46].

1.3.1 Come nasce e si sviluppa una criptovaluta: uno schema di natura enigmistica

Per comprendere il fenomeno delle criptovalute, occorre conoscere alcuni concetti noti, quali rete e nodo, e alcuni innovativi, come catena di blocchi (*blockchain*), registro (*ledger*), e blocco (*block*). La rete è un insieme di macchine direttamente collegate fra loro in forma “chiusa” (*intranet*), ovvero in forma pubblica e potenzialmente accessibile a chiunque (*internet*). Il nodo è il punto in cui pervengono, convergono e ripartono più collegamenti con altri nodi.

[44] Si osserva che le criptovalute non sono il primo esempio di moneta privata nella storia - cfr. Parlamento UE, Virtual currencies and central banks monetary policy: challenges ahead, luglio 2018.
[45] Cfr. Agenzia delle Entrate, Risoluzione n. 72/E/2016.
[46] Cfr. Agenzia Entrate, Risposta n. 14/E/2018.

Una catena di blocchi è rappresentata come una sequenza di unità collegate inscindibilmente e sempre l'una all'altra. Tali unità sono i blocchi, che confermano l'intervenuta esecuzione di una o (a seconda dei tipi di tecnologie impiegate) più *transaction*, mentre il registro è la certificazione dell'esistenza e della concatenazione di quei blocchi data dalla dispersione – ma sarebbe più corretto dire: contestuale e replicata presenza – di tutti quei blocchi su ciascuna delle macchine in rete. Un potente (e crescente) algoritmo governa, in automatico, l'intero apparato.

Per rendere più chiara la tecnologia, occorre distinguere fra i due momenti essenziali della vita di una criptovaluta: la sua creazione e il suo scambio. Momenti distinti ma correlati. Ad esempio, si supponga che il signor X voglia trasferire 10 unità di una data criptovaluta alla signora Y (magari per comprare un bene o saldare altro debito). X immetterà nel sistema (più spesso attraverso una piattaforma terza a ciò dedicata) un ordine a favore di Y attraverso una chiave crittografata[47]. Grazie all'algoritmo, il sistema risolverà il problema, ossia gestirà quell'ordine, attraverso un processo chiamato validazione: i vari computer della rete su cui è replicato il registro verificheranno che il codice immesso da X sia valido, cioè che X sia effettivamente detentore delle 10 unità da trasferire, e nel momento in cui almeno la metà più 1 dei server risponderà positivamente, il sistema riconoscerà la validità dell'operazione, generando così un nuovo blocco della catena. La *transaction* sarà quindi confermata e le 10 unità saranno trasferite alla beneficiaria Y. Perché la validazione abbia luogo occorre ovviamente che esista un precedente blocco che la comprovi (il blocco per esempio con cui X abbia comprato quelle stesse 10 unità da un terzo signor Z): l'avvenuta validazione produce, dunque, l'aggiunta del blocco alla catena che a sua volta aggiornerà il registro rendendolo, per quel blocco, del tutto immodificabile.

Ritornando alla genesi, come nasce e si sviluppa una criptovaluta, la provenienza è nel sistema stesso appena delineato. Può dirsi che, in qualche misura, il sistema di produzione sia stato elaborato in maniera esattamente speculare a quello di scambio, cioè sulla costituzione progressiva di blocchi e sul contestuale accrescimento della capacità di calcolo dell'apparato e, di conseguenza, sulla potenza di decrittazione e sulla velocità di validazione dell'algoritmo. Quest'ultimo è normalmente strutturato in funzione di una

[47] Come noto, l'incrocio di due "pezzi di codice", l'uno pubblico, altro privato, quest'ultimo qualificabile come una password che viene conservata nel computer o nello smartphone dell'utente e che serve per "firmare" l'operazione: tecnologia questa già ampiamente diffusa.

creazione di "moneta" limitata nel tempo, il che può forse consentire di prevedere, a lungo termine, un effetto complessivamente deflattivo della paravaluta, ma ancora non spiega come questa creazione abbia luogo. Ma qui si inserisce una figura di primordine nell'evoluzione espansiva della criptovaluta: l'estrattore, il minatore, il *miner*. In teoria può essere chiunque, in realtà solo soggetti che possano disporre di un elevato numero di computer e server, e che abbiano la capacità finanziaria di sopportare gli enormi costi energetici che l'estrazione comporta.

La criptovaluta nasce e si moltiplica secondo uno schema approssimativamente definito di natura enigmistica. Al minatore, che voglia aumentare la quantità di una data criptovaluta in circolazione e che si connetta al sistema con questo proposito, viene richiesta la soluzione di un "problema" (nei fatti una o più transaction) cui può pervenirsi attraverso un algoritmo alquanto complesso. Per farlo o si è autentici e assai fortunati geni universali della matematica, oppure si deve disporre di una potenza di calcolo ottenibile solo attraverso il simultaneo impiego di un gran numero di macchine che, sinergicamente, assicurino la soluzione entro un tempo ragionevolmente breve. È questo ciò che interessa al sistema "valutario" alternativo: non per mettere alla prova il minatore per uno scopo ricreativo, bensì verificare la potenza di calcolo dei mezzi di cui esso si serva. L'addizione al sistema di una simile potenza di fuoco computazionale rende più efficiente, dunque attraente e appetibile (e, apparentemente, più sicuro) l'intero apparato. La soluzione del "problema" va a costituire un nuovo blocco della catena e, in cambio di tale opera accrescitiva, il *miner* si vede riconoscere una sorta di premio (ovvero una *fee*, associata alla singola operazione) pari ad una certa nuova quantità di criptovaluta, la quale, per tale via, cresce e si moltiplica.

Ritornando alla fase di scambio, e riprendendo l'esempio precedente, si analizza la situazione dal lato dell'utente. Dunque, il Signor X non accederà direttamente alla catena dei blocchi ma lo farà attraverso una piattaforma terza. Sulla rete ve ne sono svariate che consentono l'apertura del c.d. portafoglio virtuale: è sufficiente iscriversi anche in forma del tutto anonima (la registrazione spesso richiede una mail e una password) e la piattaforma apre l'*e-wallet*. A quel punto diviene possibile acquistare criptovaluta in cambio di denaro reale. L'equivalente viene virtualmente conservato nel portafoglio, senza che tuttavia la piattaforma assuma l'obbligo di alcun rimborso: nella realtà, infatti, la criptovaluta non risiede nel portafoglio, dove invece permangono le chiavi private che servono all'utente per disporre l'operazione che poi la rete convaliderà, mentre la criptovaluta esiste soltanto in forma di registrazione nel *ledger*, e il suo spostamento da

un portafoglio all'altro non è che la risultante della sua validazione e della conseguente creazione di un nuovo blocco. Nel caso in cui l'acquirente intenda convertire la criptovaluta non potrà che rivolgersi ad una piattaforma[48], di solito (ma non necessariamente) diversa da quella che ospita l'*e-wallet*, la quale sia disponibile ad acquistare la criptovaluta (o a intermediarne la vendita presso terzi) pagandola con una valuta avente corso legale, cioè ponendo in essere un'operazione di cambio. Nel caso in cui invece l'acquirente intenda spenderla, dovrà necessariamente trovare venditori di beni o servizi disposti ad accettarla: venditori che, nella rete come nella vita reale, vanno quotidianamente aumentando.

1.3.2 Il complesso meccanismo di funzionamento delle criptovalute

Nel sistema monetario tradizionale la moneta elettronica è una disponibilità di potere d'acquisto registrata su un conto corrente acceso presso una Banca. Quando si effettua un acquisto, oppure un bonifico a favore di un beneficiario, non si verifica alcun trasferimento fisico di denaro, ma, solo, la riduzione del saldo dell'acquirente ed il contestuale aumento del saldo del venditore per un importo corrispondente. Quindi, il trasferimento si compie mediante una semplice scrittura, ed esige la partecipazione di una Banca, chiamata a verificare l'effettiva disponibilità di fondi sul conto dell'acquirente, ad eseguire l'ordine di pagamento, ad addebitare il conto dell'acquirente e ad accreditare il conto del venditore.

La moneta elettronica tradizionale richiede perciò che la tenuta dei conti sia "centralizzata", essendo indispensabile l'intervento di un ente terzo (una Banca) che, grazie ai dati custoditi nei propri server centralizzati e protetti, verifichi e confermi l'identità dell'ordinante, la disponibilità dei fondi, la correttezza dei codici di sicurezza; esegua l'operazione e la trascriva sui propri libri contabili.

Dunque, l'innovazione fondamentale portata dal Bitcoin (e dalle altre cripto-valute convertibili in circolazione) consiste proprio nell'aver superato tale esigenza di gestione centralizzata delle transazioni. Il sistema è stato, quindi, sviluppato in modo che la tenuta dei conti non sia affidata ad un unico gestore, ma distribuita tra tutti gli utenti. Il "libro contabile" su cui sono registrate tutte le operazioni non è cioè più prerogativa di una

[48] O a chiunque in rete si dichiari disponibile ad acquistarla: allo stato, infatti, non esistono limitazioni tecniche alla presenza di "cambiavalute in piazza" e, sin qui, l'incerta qualificazione giuridica del fenomeno non preclude la libera circolazione della criptovaluta.

singola Banca o del sistema bancario nel suo complesso, ma è tenuto da ciascuno degli utenti nella memoria del proprio personal computer. In tal modo, il registro non è semplicemente decentrato, ma distribuito in una rete in cui nessun "nodo" è centrale. Questo libro contabile distribuito (distributed ledger) prende il nome di blockchain. In particolare, «la blockchain si compone di una serie collegata di blocchi, i quali registrano, per ogni transazione, l'identità del corrispondente, l'importo trasferito e l'identità del beneficiario. Ciascun blocco contiene, quindi, le informazioni relative a tutte le transazioni che si sono svolte, di continuo, nell'arco di dieci minuti, nonché un riferimento al blocco precedente. Pertanto, la serie concatenata di blocchi che costituisce la blockchain fornisce in ogni istante una rappresentazione completa e aggiornata di tutte le transazioni che si sono svolte dall'avvio del sistema sino a quel momento».

In tale sistema decentrato e distribuito sono, quindi, tutti gli utenti (e non più un solo soggetto) a dover verificare la fattibilità e, pertanto, autorizzare ogni singola transazione. Precisamente, quando un soggetto effettua un ordine di trasferimento di Bitcoin (così come accade nelle normali operazioni bancarie) dovrà comunicare al sistema il proprio conto di addebito, l'importo dell'operazione ed il conto di accredito. Tuttavia, non essendo previsto l'intervento di un soggetto terzo (come un Istituto di Credito) a cui poter comunicare in via riservata le proprie chiavi di accesso al conto e che possa quindi verificare la disponibilità dei fondi, il sistema prevede che chi effettua l'operazione trasmetta agli altri utenti (ossia al sistema) una chiave di accesso al conto in forma "criptata". Per poter autorizzare l'operazione gli altri utenti saranno in conseguenza chiamati a decriptare tale chiave d'accesso attraverso la risoluzione di un complicato problema matematico, e il sistema prevede quale "stimolo premiale" che il primo soggetto che riesca a decriptare il codice ed a verificare la fattibilità dell'operazione venga ricompensato con un determinato ammontare di Bitcoin. In aggiunta, il protocollo di estrazione, oltre al conferimento del premio sotto forma di bitcoin, prevede anche delle commissioni riconosciute in capo al miner vincitori[49]. La logica è sempre la stessa, quando il codice è stato decriptato dal *miners* e l'operazione validata, la stessa verrà

[49] Attualmente il premio riconosciuto ai miner una volta validato il blocco è pari a 12,5 bitcoin mentre le commissioni sono pari a circa 0,3 bitcoin. Le prime si dimezzeranno con il passare degli anni fino al raggiungimento della soglia massima di 21 milioni. Contrariamente le commissioni invece, continueranno ad esistere anche quando finiranno i bitcoin. Per di più, data da loro quantificazione in relazione al numero di transazioni, sono destinate ad aumentare in seguito alla volontà del network di aumentare quelle attuali all'interno di un blocco con valori compresi tra 300 e 400.

inserita nel block contenente un determinato numero di operazioni, che, sommandosi ai block precedenti, darà vita appunto alla blockchain.

Alla luce di quanto esposto, va precisato che, con riferimento alle *virtual curriencies*, un ruolo determinante è certamente quello di essere valute anonime o pseudanonime. Per espresso volere dei suoi ideatori, la blockchain è, infatti, pubblica e trasparente, tanto che ogni utente della rete può visionare in qualunque momento tutte le operazioni in Bitcoin intervenute in un determinato arco temporale, il relativo importo ed i soggetti ordinante e ricevente[50]. Tuttavia, la tracciabilità delle singole operazioni non giunge sino al punto di consentire di risalire alla reale identità dei singoli operatori. Infatti, in ogni operazione ciascun user è identificato da una chiave pubblica ed una privata. Quindi, nel momento in cui si effettua un pagamento, la blockchain registra la chiave pubblica del pagante e l'importo dell'operazione, mentre la chiave privata (la password) non viene pubblicata sulla blockchain, ma rimane nella esclusiva disponibilità del titolare dell'e-wallet. Pertanto, quanto risulterà visibile sulla blockchain non sarà mai il reale nominativo di chi effettua un'operazione, ma un mero numero identificativo corrispondente alla chiave pubblica dei soggetti coinvolti. In tal senso si è appunto soliti parlare di anonimato del sistema Bitcoin, intendendosi che, pur essendo pubblico il registro delle operazioni, gli operatori non sono identificabili tramite il proprio nome e cognome, ma solo a mezzo di numeri rappresentativi della loro chiave pubblica di accesso al sistema.

Alcuni opinionisti hanno osservato come un sistema così strutturato non sarebbe in realtà idoneo a garantire l'anonimato degli operatori in valuta virtuale. A fronte di un'incertezza rispetto alla generalità dell'utente, la pubblicità della blockchain fornisce invero una completa conoscenza rispetto a tutte le operazioni generate da un determinato account, i rispettivi importi e l'account di destinazione. Nel caso in cui sulla blockchain vengano individuate operazioni sospette (si pensi ad un soggetto che ponga in essere numero elevato di operazioni, tutte dirette ad una medesima controparte in un ristretto arco temporale, o ad un soggetto che ponga in essere una singola operazione di importo estremamente rilevante), le Autorità competenti potrebbero risalire al reale titolare del conto (e-wallet) attraverso l'utilizzo di appositi *software*. Una delle principali caratteristiche del Bitcoin è, pur tuttavia, quella di offrire ad ogni utente la possibilità di generare un numero pressoché illimitato di chiavi pubbliche associate ad altrettante chiavi private, potendo così decidere di utilizzare un identificativo differente per ogni singola

[50] Il sito www.blockexplorer.com consente così di visionare in tempo reale tutte le informazioni relative alle operazioni in Bitcoin realizzate dagli utenti.

operazione realizzata. È evidente allora che, nel caso di sostituzione frequente delle chiavi crittografiche, diverrà difficile poter rinvenire elementi di sospetto nell'operatività degli users a partire dalla blockchain, e dare, quindi, avvio ad eventuali accertamenti sulle loro reali identità. Si aggiunga pure che, come ormai posto in luce da numerosi organismi nazionali ed internazionali di prevenzione e contrasto al riciclaggio, l'industria di settore sta sviluppando sistemi software sempre più complessi ed efficienti che vengono offerti agli utenti interessati e la cui finalità è proprio quella di aumentare la privacy by-passando la natura pubblica della blockchain. Il più noto è costituito dal c.d. mixing service (conosciuto anche come *tumbler*), un servizio che consente agli utenti di oscurare la cronologia delle proprie transazioni aggregando un certo numero di trasferimenti e quindi "mischiando" l'origine e la destinazione di ogni singolo pagamento[51].

1.4 Bitcoin

L'originaria forma di moneta utilizzata dal sistema blockchain è stato il Bitcoin, dando seguito al concetto e ad altre forme di criptovalute. Esso infatti, nasce simultaneamente alla tecnologia, cosa che è possibile verificare all'interno della pubblicazione del documento di Nakatomo, rappresentando di conseguenza la sua prima applicazione. Ragion per cui risulta necessaria un'accurata analisi, in modo tale da definire l'essenza stessa del fenomeno. Per cominciare, una sufficiente spiegazione è data dal sito di *bitcoinwiki.org*, gestito dalla comunità Bitcoin, secondo la quale il Bitcoin è: "*una criptovaluta elettronica decentralizzata creata da Satoshi Nakatomo nel 2008. Con il termine "decentralizzata" si intende che il Bitcoin non possiede nessun tipo di server centralizzato per l'elaborazione delle transazioni o il deposito di fondi"*. Tecnicamente sono una successione di *bit* che integra un messaggio digitale, dunque non hanno consistenza materiale come una moneta, con la funzione di consentire l'esecuzione delle transazioni *online.* Quest'ultime basate sulla logica propria delle criptovalute, ovvero il consenso tra le parti realizzato attraverso l'incrocio delle due componenti principali (chiave privata e pubblica) e il processo di validazione (secondo la modalità P2P). Il tutto affiancato dal *mining* messo in atto dai *miners*. Nella pratica, tutto ciò accade in modo

[51] Per mezzo del mixing, il pagamento da A ad A verrà perciò dirottato su B, e quello da B a B (di importo corrispondente al primo) verrà dirottato su A, in modo che risultino confusi i nominativi degli ordinanti ed i rapporti in dare e avere tra questi e i riceventi.

completamente automatico e quanto descritto è quello che si nasconde dietro un semplice click. Infatti, la procedura per ottenere e quindi acquistare un bitcoin è molto semplice: basta scaricare un programma su un cellulare o su un computer ed installarlo. A questo punto si può scegliere di diventare un *nodo full* [52] scaricando Bitcoin Core (scaricabile dal sito https://bitcoin.org/it/scarica oppure, in sede più aggiornata, https://bitcoincore.org/en/download/) o un altro *client* in grado di implementare il protocollo. Diversamente invece, si può decidere di scaricare un software gestito da un intermediario, come Coinbase (https://www.coinbase.com/?locale=it), così da creare, dopo aver effettuato le procedure di inserimento dei dati da associare al profilo, un proprio portafoglio (chiamato wallet[53]o e-wallet). Il risultato è il vantaggio della gestione diretta del portafoglio, nel primo caso, contrariamente a quanto avviene nel secondo.

Il numero di bitcoin estraibili però è limitato fino ad un massimo prestabilito di ventuno milioni, stimato entro il 2140. "*Il raggiungimento di questa soglia non farà tuttavia squillare le trombe dell'apocalisse, poiché ogni singolo bitcoin è ulteriormente dividibile fino a 10^8, ovvero un centomilionesimo di bitcoin, unità di valuta minima"*[54]. Quest'ultima è stata battezzata dalla comunità di Bitcoin, in onore del suo inventore Nakatomo, con il nome di satoshi e rappresenta l'unità di conto minima in cui può essere diviso un singolo bitcoin, che assume precisamente il valore di un cento milionesimo

[52] Per nodo full si intende un computer con istallato Bitcoin Core, così da divenire uno dei tanti nodi dove è presente il database blockchain e da partecipare quindi sia alla validazione che alla trasmissione delle transazioni ad altri nodi. In altre parole, il computer viene messo a disposizione della rete, divenendo parte della blockchain stessa. È sufficiente un computer con minimo 2 GB di RAM, spazio sufficiente ad ospitare il database (attualmente circa 350GB iniziali con un'aggiunta di circa 5/10 GB mensili) e un collegamento a internet ADSL. C'è anche la possibilità di usare una memoria esterna. Necessario invece, è rendere disponibile l'*hardware* per la rete almeno sei ore al giorno. Tale disponibilità non limita l'utilizzo del computer per altri usi propri, dunque si può usarlo contemporaneamente per svolgere qualsiasi altra operazione. Tuttavia, va detto che la piena collaborazione richiederebbe 24 ore su 24. Per maggiori chiarimenti e o approfondimenti consultare il seguente link: https://valutevirtuali.com/2019/03/14/come-aprire-un-nodo-completo-bitcoin-la-nostra-guida-introduttiva/.

[53] *Esistono vari tipi di wallet a seconda del tipo di attività che si intende svolgere e del grado di sicurezza. A) I portafogli offline, ossia portafogli hardware, sono quelli in cui l'utente è l'unico responsabile del mantenimento delle proprie monete. L'hardware detiene anche la chiave privata, cosicché questa è meno soggetta a minacce online da parte di virus e hacker, ma il portafoglio è collegato al dispositivo in cui è installato. B) per contro, nei portafogli online le chiavi private vengono memorizzate su un computer collegato a Internet. Il vantaggio è che si può accedere con qualsiasi dispositivo tramite password; lo svantaggio è che l'organizzazione che gestisce il sito detiene le chiavi private, quindi in caso di attacco hacker o di fallimento del gestore i bitcoin inseriti del portafoglio potrebbero non essere più al sicuro. C) L'ultima categoria è rappresentata dai portafogli mobili (o software); si tratta di app scaricabili sul proprio smartphone o tablet, che memorizzano le chiavi private e permettono di effettuare transazioni direttamente da questi*. In argomento https://www.cameraconsob.it/finanza/criptovalute/bitcoin-wallet/.

[54] De Collibus F. M., Mauro R., "*Hacking Finance – la rivoluzione del bitcoin e della blockchain*", Milano, Agenzia X, 2016.

dello stesso. D'altra parte, essendo l'offerta predefinita, data l'assenza di un'autorità centrale che possa modificare l'emissione, rende il bitcoin una valuta capace di sfuggire all'inflazione diversamente da quelle tradizionali. In virtù del fatto che il suo valore sia determinato da puri meccanismi di domanda è offerta. La prima è conosciuta a priori a differenza della domanda che varia in base al numero di utenti che vuole accedere attivamente alla rete[55].

Numerose sono le attività che si sono sviluppate intorno al Bitcoin, facendo nascere un vero e proprio ecosistema. Partendo dalle piattaforme di exchange e piattaforme di trading, che rispettivamente permettono di acquistare bitcoin in cambio di valute aventi corso legale oppure lo scambio on-line di criptovalute. Passando per applicazioni o attività che consentono di effettuare pagamenti direttamente in bitcoin in cambio di beni e servizi. Fino ad arrivare ad una serie, ad oggi numerose, di altre criptovalute che in alcuni casi hanno implementato elementi del Bitcoin (come Litecoin) o hanno semplicemente riprogettato il suo protocollo (come Ripple).[56]

[55] Pellizzari T., Morini M., "*il boom di Bitcoin non è per tutti"*, Il sole 24 ore, 27 novembre 2017.
[56] Si possono consultare tutte le criptovalute esistenti su https://coinmarketcap.com/.

CAPITOLO II

GLI SMART CONTRACTS NELL' INARRESTABILE EVOLUZIONE TECNOLOGICA DEGLI ULTIMI ANNI

2.1 *Smart contract:* breve rassegna

Gli smart contract sono stati oggetto di sperimentazione negli anni '90, ma l'idea di contratto intelligente si può fare risalire già agli anni '70 in relazione alla necessità di gestire l'attivazione o disattivazione di una licenza software in funzione di determinati requisiti. Uno dei primi a effettuare tali sperimentazioni e a coniare il nome stesso fu **Nick Szabo**[57]**,** un esperto di crittografia americano di origine ungheresi che grazie alla passione per la *Data Science* iniziò a ipotizzare già nel 1993, quando ancora non si parlava di *Internet of Things* e di *Big Data,* che determinati oggetti potevano essere gestiti in modo digitale in virtù di specificate condizioni.

Recentemente gli smart contract sono divenuti il fulcro di numerosi dibattiti in materia di trasformazione digitale, per gli svariati contesti in cui possono trovare applicazione, e perché rappresentano una delle molteplici dimensioni del crescente fenomeno della blockchain. Vengono definiti dal nostro regolamento – nel D.L. 14 dicembre 2018, n. 135[58], convertito in legge con L. 11 febbraio 2019, n. 12, all'art. 8-ter – come *"un*

[57] Il termine "smart contract" è stato coniato negli anni '90 da Nick Szabo, un informatico statunitense, con studi legali e di crittografia, laureatosi presso l'Università di Washington nel 1989 in informatica.
Scrive infatti Nick Szabo: "*L'idea di base dello smart contract è che molti tipi di clausole contrattuali (come la garanzia, l'assunzione dell'obbligazione, la delimitazione di un diritto di proprietà, ecc.) possono essere incorporati nell'hardware e nel software che trattiamo, in modo da rendere la violazione del contratto costosa (se desiderato, addirittura proibitiva) per il soggetto inadempiente*".
Egli, partendo dall'esempio base del distributore automatico di bevande, offre ulteriori esempi applicativi, tra cui uno, ben più "smart", relativo alla possibile gestione automatizzata dei rapporti nascenti dall'acquisto di un autoveicolo mediante pagamento a rate. Grazie, infatti, ad una combinazione di hardware e software installati nel veicolo stesso, Nick Szabo giunge ad immaginare che lo smart contract entri in azione per disabilitare la messa in moto dell'auto in caso di mancato pagamento di un certo numero di rate.

[58] Il D.L. 14 dicembre 2018, n. 135 (in GU n. 290 del 14 dicembre 2018) convertito con modificazioni dalla L. 11 febbraio 2019, n. 12 (in G.U. 12 febbraio 2019, n. 36) ed entrato in vigore dal 15 dicembre 2018, introduce nel nostro ordinamento giuridico le nozioni di tecnologie basate su registri distribuiti e smart contract.
Dispone infatti l'art. 8-ter del decreto:

programma per elaboratore che opera su tecnologie blockchain e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse". È necessario inoltre che *"soddisfino il requisito della forma scritta previa identificazione informatica delle parti interessate".*

Con questo concetto si intende la trascrizione e traduzione di un contratto, contenente delle condizioni che devono essere rispettate per fare sì che le definizioni operative possano essere compiute. La logica che viene rispettata è quella del *"if-this-then-that"*[59], ovvero "se questo accade allora succede". Ne consegue che il supporto legale è, quindi, di utilità nella stesura dello smart contract, ma non nella fase di verifica e attivazione, che avviene in maniera automatica.

Le maggiori differenze tra gli smart contract e i contratti disciplinati dal Codice civile sono:

- nei normali contratti la fiducia viene garantita da una figura terza, che può essere quella di un notaio o di un avvocato. Nello smart contract, il ricorso ad una figura terza viene meno. Risulta tuttavia chiaro che alcune garanzie debbano essere comunque sempre rispettate: il codice non deve essere modificabile, le basi e fonti dati devono essere provate ed affidabili, e le modalità di lettura e controllo delle fonti dati devono essere certificate;

"*1. Si definiscono "tecnologie basate su registri distribuiti" le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili.*

2. Si definisce "smart contract" un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse. Gli smart contract soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con linee guida da adottare entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto.

3. La memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui all'articolo 41 del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014. 4. Entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto, l'Agenzia per l'Italia digitale individua gli standard tecnici che le tecnologie basate su registri distribuiti debbono possedere ai fini della produzione degli effetti di cui al comma 3".

Detto articolo definisce quindi le nozioni di "tecnologie basate su registri distribuiti" al primo comma e di "smart contract" al secondo, prevedendo al terzo comma gli effetti giuridici della memorizzazione di un documento informatico attraverso l'uso di tali tecnologie basate su registri distribuiti.

[59] Il linguaggio di cui si compongono i codici dei software è di estrema semplicità e viene generalmente espresso secondo lo schema di carattere binario IFTTT ovvero "*if this than that*" (letteralmente: "se questo allora quello"). Secondo tale schema, al verificarsi di un determinato evento il software riconnette l'esecuzione di un'azione specifica. È proprio l'estrema semplicità della struttura del codice, che oltretutto sembrerebbe idonea a conferire maggiore certezza in fase di esecuzione del rapporto, a rendere lo *smart contract* particolarmente appetibile per le parti.

- negli smart contract non c'è spazio alla violazione delle condizioni sottoscritte, dal momento che tra le loro caratteristiche intrinseche ci sono proprio l'esecuzione automatica e l'inalterabilità.

L'accordo negoziale (1325 c.c.), che rappresenta uno dei requisiti essenziali del contratto stesso (1321 c.c.), rimane in capo alle rispettive parti. Dovrà esserci, come nei normali contratti, una perfetta coincidenza tra la volontà delle parti, che dovrà essere tradotta in codice.

Diversi possono essere i vantaggi derivanti dall'uso degli smart contract:

- indipendenza da intermediari[60], quali notai e avvocati, nella fase di verifica ed approvazione del contratto;
- immodificabilità del codice, che esclude l'esigenza di figure terze che esaminino la liceità e validità di un accordo;
- risparmio economico, dovuto in gran parte all'esclusione di intermediari nelle fasi di verifica e approvazione;
- maggiore precisione e riduzione degli errori, poiché lo smart contract, in modo automatico, al verificarsi delle condizioni stabilite, fa sì che si verifichino determinate azioni;
- genericamente, semplificazione delle operazioni di contrattazione.

Tuttavia, oltre a diversi vantaggi emergono anche alcuni elementi da monitorare con attenzione:

- linguaggio in codice: è necessario che le parti si affidino da un lato ad un esperto informatico in grado di tradurre in codice il testo dell'accordo, dall'altro a figure intermediarie atte alla corretta trasmissione della volontà delle parti alla figura informatica, al fine di evitare equivoci o incomprensioni, che comprometterebbero la reale volontà delle parti;

[60] Sebbene non sia corretto affermare che gli smart contracts possano mettere in discussione il ruolo di tali figure, al contrario però, è lecito immaginare che imporranno a studi legali o notarili un adeguamento che sia in grado di coniugare le novità apportate nella realizzazione di contratti, fortemente innovativi, con il complesso di principi ed istituti giuridici fondamentali dell'ordinamento. Risulta quindi, un'ardua e non remota sfida che questi professionisti si troveranno ad affrontare con espetti come il linguaggio in codice, l'interpretazione del contratto e l'esecuzione automatica della prestazione, elementi di criticità non solo per loro ma anche per gli stessi smart contracts.

- interpretazione del contratto (relativa a intenzione dei contraenti, interpretazione complessiva delle clausole, interpretazione di buona fede, ecc.).
- esecuzione automatica della prestazione: non lascia la possibilità per i contraenti di compire azioni contrarie o diverse da quelle previste nelle clausole contrattuali, limitando il potere discrezionale delle parti. Può quindi creare delle difficoltà per quanto riguarda l'irrevocabilità dell'accordo e quindi all'applicabilità di istituti quali: recesso, annullabilità, nullità, risoluzione.

L'art. 1321[61] c.c. definisce il contratto come "l'accordo di due o più parti per costituire, regolare, o estinguere tra loro un rapporto giuridico patrimoniale". Oltre all'aspetto patrimoniale, legato quindi alla valutazione/natura economica, gli smart contract per il diritto italiano, devono rispettare altri requisiti prescritti dall'art. 1325 c.c.: l'accordo, le parti, la causa, l'oggetto e la forma. Tra questi requisiti, la forma scritta è quello che suscita maggiori perplessità. La forma scritta trova la sua ragione di essere per due principali motivi:

- *Ad substantiam*: la forma è richiesta per la validità stessa dell'atto.
- *Ad probationem*: la forma costituisce l'unico mezzo per provare l'esistenza di quel negozio.

La questione della forma scritta nei documenti informatici è stata affrontata dal Decreto Legislativo 13 dicembre 2017 n. 217, recante le modifiche e le integrazioni al "Codice dell'Amministrazione Digitale."

L'art. 20 del suddetto Decreto sancisce che il documento informatico soddisfi il requisito della forma scritta e abbia l'efficacia di cui all'art 2720 c.c. ("piena prova" della provenienza delle dichiarazioni da chi ha sottoscritto il documento salvo un

[61] Il contratto è definito dall'art. 1321 c.c. come "*l'accordo di due o più parti per costituire, regolare o estinguere tra loro un rapporto giuridico patrimoniale*". Elementi essenziali del contratto, a norma del successivo 1325 c.c., sono: l'accordo delle parti, la causa, l'oggetto e la forma (quest'ultima quando prevista dalla legge a pena di nullità).
Ripercorrendo, brevemente, tali elementi:
* le parti (o centri di interessi): sono i soggetti rispetto ai quali, o nel cui interesse, il contratto esplica le conseguenze giuridiche pattuite;
* l'accordo: è l'incontro della volontà delle parti ed è quel "quid" essenziale che dà vita al contratto;
* la causa (la cui definizione non sempre è univoca): può essere genericamente indicata come l'elemento giustificativo che rende giuridicamente apprezzabile lo scopo a cui tende in concreto l'attività delle parti;
* l'oggetto (concetto anch'esso non univoco): rappresenta l'insieme delle prestazioni e, quindi, qualunque cosa le parti siano tenute a fare a non fare o a dare.
Ultimo, ma non per importanza, è il requisito della forma.

disconoscimento da quest' ultimo) qualora sia sottoscritto con una firma digitale, qualificata o avanzata, o, nel caso di documenti sottoscritti con firme elettroniche differenti, qualora rispetti gli standard tecnici individuati dall'AgID (con modalità volte a garantire sicurezza, integrità, immodificabilità del documento e riconducibilità dell'autore). Nei restanti casi il valore probatorio del documento informatico è rimesso al libero giudizio degli organi giudicanti.
Altri elementi di interesse sono il tema dell'identificazione del firmatario (e le relative modalità in cui questo può avvenire, come per esempio, con la firma elettronica, o con l'uso di SPID) per cui l'AgID sta definendo dei requisiti idonei a far sì che un processo di identificazione informatica possa dar luogo alla creazione di firme elettroniche. Un altro tema da gestire e regolamentare è quello della responsabilità civile, dal momento che l'intervento umano è limitato: la scrittura del codice è infatti in grado di fare scaturire delle conseguenze in seguito al verificarsi di determinate condizioni.

Senza tralasciare le problematiche relative alle clausole vessatorie, disciplinate dal Codice civile e dal Codice del consumo, che rappresentano un ulteriore criticità in termini di tutela del contraente più debole. Partendo dal presupposto che una clausola all'interno di un contratto è una parte del regolamento contrattuale, di conseguenza il suo effetto è quello di essere vincolante. Diviene di fatto, un obbligo sancito dal contratto. Tuttavia, spesso i contratti sono frutto dell'elaborazione unilaterale da parte di un soggetto che predispone schemi contrattuali uniformi, destinati ad operare nei confronti della generalità della clientela, prescindendo dunque da una reale trattativa negoziale.[62] Ipotesi dei contratti in serie, conclusi mediante moduli o formulari (art. 1342 c.c.), o con condizioni generali di contratto (art. 1341 c.c.). Casi in cui al contraente, che ha espresso la sua volontà di accettare il regolamento contrattuale attraverso la sottoscrizione, è di fatto preclusa ogni possibilità di modificare lo schema contrattuale già preventivamente elaborato dalla controparte.[63] In aggiunta, subisce l'efficacia delle clausole, non solo quando le ha espressamente accettate, ma anche quando, pur in mancanza di espressa accettazione, egli le ha conosciute o avrebbe dovute conoscerle usando l'ordinaria diligenza. Nei contratti con condizioni generali di contratto le clausole sono predisposte unilateralmente dal contraente più forte, tipicamente sono di limitazione delle garanzie e declino della responsabilità, e la volontà del contraente più debole è ridotta al minimo, al

[62] Tupponi M., "*Manuale di diritto commerciale internazionale"*, G. Giappichelli Editore, Torino, 2019.
[63] Ibidem.

solo accettare o rifiutare. In sostanza, sono clausole chiamate "vessatorie" particolarmente sfavorevoli, sia da un punto di vista economico che giuridico. A tal riguardo, l'ordinamento nazionale prevede due diverse discipline: il Codice civile, se si tratta di clausole vessatorie in contratti B2B e il Codice del consumo, in caso di contratti B2C. Ad ogni modo, sono disposizioni volte alla tutela del contraente più debole, quindi rispondono prontamente a logiche di difesa in un rapporto contrattuale non equo, dove la parte più forte impone la propria volontà. Risultano innegabili le limitazioni che potrebbero sorgere quando si parla di smart contract, ma d'altra parte, considerando un contesto ideale, si potrebbe risolvere il problema alla radice attraverso il consenso distribuito.

Il loro impiego infatti, è oggi ancora limitato ma la loro diffusione in contesti dominati dalle nuove tecnologie, dove automazione e velocità di esecuzione sono un vero fattore differenziale e di cui i network blockchain sono un chiaro esempio, li pone al centro dell'attenzione della normativa nazionale ed internazionale.

2.2 Gli *smart contract* nel paradigma della blockchain

Dopo l'introduzione di bitcoin, si è studiata la possibilità di allargare lo schema della blockchain oltre l'originario ambito criptovalutario, verso scenari applicativi formalmente suscettibili di un'estensione quasi generalizzata. In questo senso, viene da più parti affermato che le tecnologie e i modelli di funzionamento sottostanti la blockchain potrebbero astrattamente investire le dinamiche gestionali e di scambio di qualsiasi bene, valore o informazione rappresentabile digitalmente. Gli sviluppi attuali sono il frutto di un articolato processo evolutivo che origina dal concetto di *Distributed Ledger Technology* (*DLT)* [64] e di blockchain.

All'inizio, si è pensato di estendere le caratteristiche del sistema bitcoin allo scopo di collegare alla disponibilità di una specifica unità di criptovaluta la titolarità di un diverso asset digitale, o di un diritto su un bene esistente nel mondo fisico. Attraverso questo

[64] Il termine 'DLT', o Distributed Ledger Technologies (tecnologie a registri distribuiti), indica un insieme di protocolli che permettono ad una rete composta da nodi di attori di pari entità (*peer nodes*) di gestire un registro, o ledger, sincronizzato tra i partecipanti grazie all'utilizzo della crittografia e senza necessità di un unico nodo centrale che si occupi della gestione e del controllo del registro.

espediente è possibile, ad esempio, associare una specifica ed individuale criptounità al diritto di proprietà sopra un determinato bene, quale può essere un'autovettura. In tal modo, la proprietà del veicolo seguirà astrattamente le vicende traslative dell'unità criptomonetaria che la rappresenta all'interno della blockchain. Certamente, tale tipo di impostazione presenta dei limiti sostanziali: infatti, mentre la circolazione delle criptomonete avviene all'interno di un sistema autosufficiente ed autoreferenziale (nel senso che esse esistono soltanto all'interno di un registro distribuito, che presiede e certifica tutti i loro trasferimenti); lo stesso non può certo affermarsi con riferimento ad entità esterne alla blockchain, le quali seguono le regole, anche giuridiche, del mondo reale.

Successivamente, sono stati studiati modelli più evoluti. Sotto una diversa angolazione, infatti, è possibile delineare la blockchain come un'architettura di elaborazione distribuita, composta da una pluralità di nodi che eseguono, registrano e verificano le medesime operazioni. Nel caso della Blockchain bitcoin, la tipologia di operazioni computabili dal sistema è sostanzialmente limitata al trasferimento di una determinata quantità di criptomoneta da un soggetto ad un altro: ciò in ragione della scarsa flessibilità del linguaggio di programmazione alla base di tale blockchain, dimostratosi inadatto ad esprimere rapporti più complessi. Tuttavia, con il crescere di importanza del fenomeno, si sono esaminati nuovi modelli di funzionamento, allo scopo di estendere gli scenari attuativi della tecnologia.

L'esempio che, probabilmente più di ogni altro, appare in grado di esprimere questa tendenza evolutiva è rappresentato da '*ethereum'*: una blockchain programmabile che permette ai suoi utilizzatori di coniugare i benefici in termini di disintermediazione, sicurezza, automazione ed irreversibilità delle transazioni, propri di un sistema fondato sul concetto di blockchain, con l'elasticità offerta da un linguaggio di programmazione *Turing* equivalente.

Ethereum, in pratica, rappresenta una piattaforma attraverso la quale è possibile creare e far eseguire automaticamente, da una macchina virtuale distribuita (la c.d. *Ethereum Virtual Machine*), operazioni di qualsiasi genere, aventi o meno rilevanza economica, il cui contenuto e grado di complessità è quasi totalmente rimesso all'iniziativa degli utenti. Il riferimento al modello *Ethereum* consente di approssimarsi a ciò che costituisce il nucleo soprattutto innovativo delle blockchain di nuova generazione, nonché l'elemento che le rende atte ad essere utilizzate per finalità eterogenee: lo smart contract.

Dunque, il meccanismo di funzionamento di una qualsiasi blockchain può essere scomposto fino ad identificare quella che descrive la funzione più basilare svolta dal sistema e, cioè, l'esecuzione e la registrazione di transizioni di stato in un contesto decentralizzato, reso affidabile dall'utilizzo della crittografia e del consenso distribuito.

La tipologia di transizioni di stato gestibili dalla blockchain bitcoin è essenzialmente circoscritta all'ambito del trasferimento di bitcoin da un account ad un altro. Tale limitazione, tuttavia, non è intrinsecamente connaturata all'idea di blockchain, ed il suo superamento è, appunto, l'obiettivo conseguito mediante lo strumento degli smart contract. La notevole flessibilità del linguaggio di programmazione della *Ethereum Virtual Machine* consente a ciascun utente di creare smart contract in grado di codificare e computare qualsiasi funzione di transizione di stato: in altre parole, può affermarsi che tramite un singolo smart contract, ovvero attraverso una pluralità coordinata di contratti "intelligenti", è astrattamente possibile riprodurre e far eseguire dal sistema (in via autonoma) ogni genere di operazione o rapporto economico-patrimoniale, riconducibile in forma algoritmica. Ferme restando, chiaramente, le ineliminabili approssimazioni e rigidità proprie del codice informatico ed il collegamento necessariamente mediato tra quanto risulta certificato all'interno della blockchain e la realtà del mondo analogico.

2.3 *Smart contract* e contratti 'tradizionali'

Lo *smart contract*, o 'contratto intelligente', è stato per la prima volta definito, in termini non giuridici, come *"un insieme di promesse* (in linea con il concetto di contract anglosassone), *espresse in forma digitale, incluse le regole che le parti vogliono applicarvi"*. Ma giuridicamente più attinente è la definizione che inquadra gli smart contract in *"un accordo automatizzato ed eseguibile. Automatizzato da un computer, sebbene alcune parti richiedano un input o un controllo umano. Eseguibile sia attraverso il ricorso all'autorità giudiziaria che tramite l'esecuzione automatica del codice"*. Dunque, un contratto intelligente consiste in un insieme di clausole, espressione di un accordo tra due o più parti, che sono programmate in codice alfanumerico. Il "codice" rappresenta un set di istruzioni con la descrizione di condizioni al verificarsi delle quali vengono automaticamente attivate specifiche azioni, anche esse definite nel codice. Il

codice viene conservato sul blockchain, così come le transazioni sono preservate normalmente su altre catene di controllo.

Il segnale che determina l'esecuzione delle istruzioni registrate nello smart contract può dipendere da variabili interne allo stesso, e cioè dalla successione di avvenimenti già compresi nel codice (come, ad esempio, lo spirare di un termine) ovvero da circostanze esterne (per esempio, un tasso di interesse). In tale seconda ipotesi è necessario l'intervento di un elemento esterno al blockchain (c.d. 'oracolo') che costituisce un collegamento tra la catena e il mondo reale, e permette la verifica del soddisfacimento delle condizioni esterne. L'oracolo può essere strutturato anche per interrogare più fonti al fine di accertare il verificarsi di fattori esterni alla catena (ad esempio, un *data feed* che fornisce un tasso di interesse, un sensore che trasmette dati atmosferici quali temperatura e umidità, un GPS che trasmette una posizione, oppure un organismo terzo che gestisce un conflitto). L'oracolo è una fonte di dati affidabile e certificata che fornisce sostegno per l'esecuzione (o la non esecuzione) dello smart contract, inviando al blockchain informazioni relative al mondo reale, che riguardano circostanze dedotte nel codice, quali presupposti per l'esecuzione del contratto.

A differenza di una catena di controllo semplice che registra solo le transazioni, lo smart contract aggiunge un codice autoeseguibile con un ulteriore grado di complessità e di organizzazione. I protocolli verificano ed eseguono le clausole del contratto, e monitorano l'esecuzione dello stesso. La tecnologia blockchain permette, quindi, per così dire, la *selfenforceability d*el contratto: vengono cioè eseguiti automaticamente i termini e le condizioni dello stesso al verificarsi degli eventi predeterminati dalle parti e iscritti nel codice.

Gli smart contract si fondano, come un diagramma di flusso, sulla logica *"if this then that":* una volta soddisfatte le condizioni descritte nel codice si attivano automaticamente delle specifiche azioni che non possono essere interrotte. Infatti, dato che il libro mastro di blockchain è immutabile, il codice - e così il contratto al quale esso si riferisce - può solo essere cancellato o modificato seguendo i termini definiti dal codice stesso. Pertanto, a differenza dei contratti tradizionali, che offrono la possibilità di adempiere le prestazioni come stabilito nel contratto stesso o di rendersi inadempienti ed andare incontro alle relative conseguenze (ad esempio, sospensione della controprestazione, risoluzione per inadempimento, ecc.), tale opzione non è disponibile in uno smart contract dove

l'adempimento del contratto è, per così dire, automatizzato e subordinato unicamente al verificarsi di determinati eventi sottratti alla volontà delle parti[65].

L'adempimento 'automatico' di uno smart contract è armonico alle teorie "non negoziali" che sottolineano l'irrilevanza dell'animus solvendi nell'inquadramento del concetto di adempimento[66].

In sostanza, è possibile descrivere lo smart contract come un contratto:

- digitale: le clausole contrattuali sono incorporate nel software sotto forma di codice;
- autoeseguibile: l'adempimento, essendo governato dagli input previsti nel codice, prescinde non solo dall'animus solvendi del debitore, ma finanche dal comportamento delle parti;
- irrevocabile: una volta iniziato, il processo di esecuzione non può essere fermato o modificato.

Da tali caratteristiche discendono diversi vantaggi che contraddistinguono il contratto intelligente rispetto a quello 'tradizionale'. In primo luogo, per quei contratti che richiedono la necessaria partecipazione di un terzo intermediario (come, ad esempio, la fornitura di energia elettrica e gas, la stipula di polizze assicurative, la compravendita di un bene immobile, la concessione di una linea di credito, ecc.) la conclusione di un contratto sul blockchain sostituisce la necessità di un terzo intermediario con una 'validazione' distribuita, con conseguente risparmio di tempo e di riduzione di costi normalmente legati all'adempimento dell'accordo contrattuale e ciò riduce (se non azzerare del tutto) il rischio di inadempimento di controparte. In aggiunta, la registrazione (irreversibile e immodificabile) dello smart contract sul blockchain, lascia una traccia indelebile e trasparente della storia del bene oggetto del medesimo e diminuisce il rischio di danni derivanti da errori e frodi.

Per queste ragioni, vi sono molteplici progetti in svariati settori ove si sperimenta l'applicazione pratica degli smart contract. Per esempio, gli smart contract possono essere utilizzati nella fornitura e nel pagamento di energia elettrica: al consumo registrato dal contatore (che, in questo caso, rappresenta l'oracolo che collega il codice alla realtà

[65] Per tale motivo lo *smart contract* è stato accostato più volte alle cc.dd. *vending machine* (distributori automatici), dove, una volta innescato il processo mediante l'inserimento del denaro e la digitazione del codice prodotto, l'adempimento (i.e. l'erogazione del prodotto) è automatico e irreversibile.

[66] Contraria a tale interpretazione è la teoria negoziale, secondo cui l'adempimento, per poter essere qualificato tale, deve essere accompagnato da una specifica volontà del debitore di adempiere (cioè dell'*animus solvendi*) e dall'accettazione del creditore.

esterna) ne consegue una bollettazione precisa ed un puntuale pagamento della fattura. Un secondo esempio è rappresentato dalla piattaforma UjoMusic, che permette agli utenti di ascoltare musica e utilizzare i registri distribuiti per pagare direttamente gli artisti, senza ricorrere ad alcun tipo di intermediario. Infine, una ulteriore applicazione pratica dei contratti intelligenti in via di sviluppo riguarda la vendita di beni a rate: in una vendita a rate di un'autovettura, ad esempio, è stata ipotizzata una codificazione contrattuale che permette di avviare il motore solo dietro il pagamento della rata nel termine pattuito[67].

2.3.1 Natura e interpretazione[68] dello smart contract

Un primo tema controverso relativo ai contratti intelligenti riguarda la natura giuridica. In particolare, ci si è interrogati circa la relazione che intercorre tra l'accordo contrattuale e il protocollo informatico o codice sotteso allo smart contract. Da un lato, infatti, si potrebbe sostenere che gli smart contract siano in grado di sostituirsi completamente ai contratti tradizionalmente intesi e che il codice che si traduce nello smart contract costituisca, in toto, il contratto.

Il codice, secondo tale interpretazione, avrebbe forza di legge tra le parti ai sensi dell'art. 1372 c.c. e sarebbe, quindi, autosufficiente, autoeseguito e autoimposto, con la conseguenza - francamente eccessiva - che gli smart contract potrebbero porsi al di là di ogni possibile controllo da parte degli stati nazione e della relativa giurisdizione legale. Ritenere che il codice sia legge equivarrebbe, infatti, ad affermare che qualsiasi errore,

[67] Un tale schema si colloca nell'alveo delle diverse forme di autotutela previste nell' ordinamento italiano, quali, ad esempio, l'eccezione di inadempimento ex art. 1460 c.c., il potere di sospendere l'esecuzione in caso di mutamento delle condizioni patrimoniali di controparte ex art. 1461 c.c., e il diritto di ritenzione previsto dagli artt. 2756 e 2761 c.c.

[68] Problematiche emergono con riferimento all'interpretazione del contratto, posto che tale operazione si pone come necessario presupposto logico dell'esecuzione, operazione, quest'ultima, cui il software dovrebbe provvedere automaticamente. Il Codice civile italiano prescrive una serie di criteri (Libro IV, Capo V, artt. 1362- 1371) cui conformarsi nell'interpretazione del contratto. È prassi distinguere tra criteri di interpretazione soggettiva (e.g. artt. 1362 e 1363) e criteri di interpretazione oggettiva (artt. 1366 e 1367). Risultano di tutta evidenza problematiche di tipo applicativo con riguardo a canoni di carattere soggettivo. Si pensi all'interpretazione del contratto secondo la comune intenzione delle parti o secondo il comportamento complessivo delle stesse. Infatti, se nel primo caso si richiede di procedere all'accertamento di un elemento la cui stessa esistenza potrebbe peraltro pure discutersi, nel secondo è richiesta la considerazione di elementi che debbono necessariamente porsi al di fuori del testo contrattuale. Entrambe le ipotesi richiedono comunque il compimento di operazioni che allo stato attuale non sembrano essere eseguibili in via del tutto automatica da parte di un software. Ma neppure le regole rientranti tra i criteri oggettivi, quali ad esempio l'interpretazione secondo buona fede (art. 1366) ed il principio conservativo (art. 1367) o dell'interpretazione *contra stipulatorem* (art. 1370), sembrano, in ragione della complessità delle operazioni di valutazioni richieste, potersi eseguire da un software in totale autonomia.

clausola illegale o mancato recepimento di norme imperative diventerebbe parte del contratto, rendendo lo stesso scollegato da ogni tipo di controllo esterno.

Argomentando in modo diametralmente opposto, invece, si potrebbe ridurre il ruolo degli smart contract alla mera automazione dell'adempimento sulla scia di quanto avviene nel settore delle *vending machine.*

Secondo tale interpretazione, il vantaggio che conseguirebbe all'utilizzo dei contratti intelligenti sarebbe limitato unicamente alla digitalizzazione e all'automatizzazione dell'adempimento al verificarsi di determinati eventi.

Un'interpretazione più realistica degli smart contract, che ne coglie il più ampio potenziale, li colloca all'interno del sistema giuridico tradizionale, sottolineando una discrepanza tra l'accordo delle parti e il protocollo codificato e, dunque, l'esigenza che gli smart contract debbano necessariamente integrarsi con ulteriori elementi espressione dell'intenzione e della volontà delle parti. Questa interpretazione (c.d. *split contracting model*) se da un lato, infatti, riconosce che gli smart contract possono determinare un aumento di efficienza in molti settori (con conseguenti riduzioni di costi di transazione e, ad esempio, dei tempi necessari per lo svolgimento di attività di verifiche o controlli), dall'altro pone l'accento sull'incapacità e la difficoltà di tradurre in un unico codice complesse strutture negoziali.

Seguendo tale ragionamento, si comprende, dunque, come lo smart contract afferisca non alla fase di formazione del contratto, che è e resta costituita dall'accordo tra le parti, ma a quella dell'adempimento, con la conseguenza che lo smart contract non integrerebbe neppure una fattispecie di contratto atipico ai sensi dell'art. 1322 c.c. Peraltro, se, da un lato, l'autonomia contrattuale è preservata in relazione al momento di formazione del contratto, dall'altro lato la stessa viene limitata in relazione alla fase dell'adempimento. Sono, infatti, sottratti alla volontà e al controllo delle parti e di soggetti terzi (e, teoricamente, anche all'immediato sindacato del giudice) gli elementi afferenti all'adempimento del contratto che vengono attuati automaticamente al verificarsi delle condizioni prestabilite e inserite nel codice[69].

Altro tema aperto in relazione agli smart contract è quello relativo all'interpretazione dei contratti intelligenti. Ridurre uno smart contract al codice determinerebbe l'eliminazione di qualsivoglia spazio per l'interpretazione. Infatti, se gli smart contract consentono

[69] Da una diversa prospettiva, si potrebbe inquadrare lo smart contract come una forma atipica di autotutela, alla luce del fatto che l'esecuzione automatizzata tutela il privato dall'inadempimento contrattuale di controparte.

l'adempimento automatico secondo regole programmate sottese ciò per cui sono programmati, non potrebbero trovare applicazione le regole ermeneutiche di cui agli artt. 1362 - 1371 ss. c.c. che, nel caso dei contratti 'tradizionali', sono utilizzate per la ricerca della comune intenzione delle parti contraenti al momento della conclusione del contratto, talvolta nascosta dietro il significato oscuro o ambiguo delle espressioni utilizzate nel testo contrattuale. Alcune locuzioni giuridiche "qualitative" (ad esempio, buona fede) difficilmente possono essere tradotte nel linguaggio dei codici impiegato negli smart contract e richiedono necessariamente un intervento dell'interprete che tenga conto del settore di applicazione e della tipologia contrattuale. Anche sotto questa prospettiva, dunque, occorre che gli smart contract possano agganciarsi ad un elemento esterno. Al pari di tutti i contratti, anche l'interpretazione degli smart contract deve quindi tenere conto dei criteri dettati dalle previsioni codicistiche di cui sopra e, in particolare, non può sottrarsi ad uno dei principi cardine del nostro ordinamento, sancito dall'art. 1366 c.c., ossia l'obbligo di interpretare il contratto secondo buona fede.

2.3.2 Formazione del contratto

Altro tema che merita attenzione è quello relativo alla fase di formazione del contratto. Se, infatti, lo smart contract fa salva l'autonomia delle parti nella fase di formazione del consenso e, al pari di qualsiasi contratto, consiste in una manifestazione di tale volontà, può verificarsi che la formalizzazione di tale volontà manifestata esternamente non corrisponda al vero intento negoziale del dichiarante. Come noto, il nostro ordinamento considera e disciplina tali scenari, prevedendo che i contratti conclusi da un contraente il cui consenso sia stato dato per errore, estorto con violenza o carpito con dolo possano essere annullati su richiesta del medesimo contraente alle condizioni di cui agli artt. 1427 ss. c.c., ossia quando l'errore è essenziale ed è riconoscibile dall'altro contraente (art. 1428 c.c.), quando la violenza prospetta un male ingiusto e notevole (art. 1435 c.c.) o quando il dolo è determinante per la conclusione del contratto (art. 1439 c.c.)[70].
Inoltre, a tutela di soggetti considerati particolarmente vulnerabili dall'ordinamento, il codice civile, all'art. 1425, sancisce anche l'annullabilità del contratto concluso

[70] Al riguardo, per gli smart contract potrebbe assumere particolare importanza la disciplina sul c.d. errore ostativo di cui all'art. 1433 c.c. che, consentendo l'annullamento del contratto quando l'errore riguarda non la formazione, ma la comunicazione della volontà, porrebbe un rimedio per tutte quelle situazioni in cui il codice non trasponga correttamente la volontà delle parti.

dall'incapace legale e, in presenza delle condizioni di cui all'art. 428 c.c., dall'incapace naturale. Tuttavia, se tali meccanismi di tutela trovano normale applicazione con riferimento ai contratti tradizionali, occorre invece interrogarsi circa la loro possibile applicazione agli smart contract qualora ricorrano le condizioni allo scopo previste dall'ordinamento.

Ulteriori problemi in relazione alla capacità di agire e corretta formazione della volontà contrattuale riguardano la possibilità di verificare l'identità della parte contraente. Infatti, esaminate le caratteristiche degli smart contract, è evidente che gli stessi non possano essere ricondotti facilmente a una persona fisica o giuridica, considerata la possibilità di agire in via anonima o sotto pseudonimi.
Da ciò consegue la difficoltà di riuscire a stabilire se le parti contraenti avessero o meno la capacità d'agire al momento della conclusione del contratto e se la relativa volontà contrattuale sia stata eventualmente viziata.
Pertanto, nonostante sia ormai indiscussa la possibilità di concludere contratti, e quindi anche contratti intelligenti, per via informatica tenuto conto della diffusione sempre maggiore del commercio elettronico, non si può escludere il rischio che il codice non contenga una corretta trasposizione della volontà della parte contraente e vi siano differenze tra l'accordo contrattuale e la traduzione nell'algoritmo.

2.3.3 Forma del contratto

Un ulteriore tema da considerare in merito all'utilizzo degli smart contract è quello relativo alla applicabilità agli stessi dei requisiti formali (*ad substantiam* o *ad probationem*) dettati dal nostro ordinamento. Il D.lgs. 7 marzo 2005[71], n. 82 in relazione

[71] Gli artt.20 comma 1-bis e 21 comma 2-bis Decreto Legislativo 5 marzo 2005, n. 82 rispettivamente dispongono:
"*Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità.*".
e:
"*Salvo il caso di sottoscrizione autenticata, le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del Codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale. Gli atti di cui all'articolo 1350, numero 13), del Codice civile redatti su documento informatico o formati attraverso procedimenti informatici sono*

ai documenti informatici[72] riconosce che gli stessi se sottoscritti, *inter alia*, con firma digitale basata su un sistema di chiavi crittografiche, una pubblica e una privata, integrano il requisito della forma scritta e l'efficacia probatoria prevista dall'art. 2702 c.c. Si potrebbe far leva sull'utilizzo del meccanismo di crittografia a chiave asimmetrica ad opera dei fruitori del blockchain per riconoscere anche allo smart contract il requisito della forma scritta e l'efficacia di piena prova sino a querela di falso ai sensi della menzionata previsione codicistica.

2.3.4 Adempimento del contratto

Nonostante l'adempimento nei contratti intelligenti sia automatizzato, potrebbero sorgere contestazioni tra le parti in merito all'esattezza dell'adempimento. Nel nostro ordinamento la previsione cardine su questo tema è rappresentata dall'art. 1375 c.c., che impone alle parti di eseguire il contratto secondo buona fede: interpretando ed applicando tale disposizione, la Suprema Corte ha più volte affermato che, in presenza di talune circostanze, anche un'esecuzione perfettamente aderente alla lettera del contratto (come nel caso dell'esecuzione automatica dello smart contract) potrebbe costituire nei fatti un inadempimento perché contraria al canone generale della buona fede.
Sul punto, non manca chi sostiene che tali problemi possano essere affrontati predeterminando criteri precisi nel codice e, quindi, sottraendo alle parti ogni margine di discrezionalità valutativa. Tale soluzione, tuttavia, non pare del tutto soddisfacente, in quanto difficilmente possono essere predeterminati ex ante tutti i criteri necessari ad escludere del tutto la necessità di una valutazione qualitativa. Più condivisibile sembra, invece, essere la posizione di coloro i quali ritengono che tali questioni debbano essere risolte, anche con riferimento agli smart contract, attraverso i metodi tradizionali di risoluzione delle controversie.

2.3.5 Integrazione e esecuzione forzata del contratto

Occorre interrogarsi circa i rimedi attivabili qualora i contratti intelligenti si pongano in contrasto con norme di ordine pubblico o norme imperative.

---

sottoscritti, a pena di nullità, con firma elettronica avanzata, qualificata o digitale ovvero sono formati con le ulteriori modalità di cui all'articolo 20, comma 1-bis, primo periodo.".

[72] I documenti informatici sono da intendersi come i documenti elettronici che contengono la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Come noto, le norme cogenti trovano applicazione indipendentemente dalla volontà dei singoli (ad esempio, sono nulle pattuizioni che hanno l'effetto di privare il consumatore di determinate protezioni derivanti dal codice del consumo). Analogamente, in caso di controversie relative al contratto, l'esecuzione può essere ottenuta attraverso l'intervento di organi giudiziari che, definita la controversia, possono altresì imporre l'esecuzione in forma specifica delle obbligazioni ovvero il risarcimento dei danni.

Considerato che gli smart contract non sono modificabili e l'adempimento è automatico, si discute se sia possibile ottenerne l'esecuzione o la risoluzione senza la necessità di coinvolgere organi terzi. Anche a tale riguardo non manca chi sostiene l'assoluta indipendenza degli smart contract dagli impianti tradizionali, ritenendo che pure le fasi patologiche del rapporto si possano affrontare traducendo nel codice, altresì, le 'reazioni' ad azioni/inadempimenti predefiniti.

In tal senso, l'automazione dell'esecuzione del contratto intelligente è euritmica ai casi di autotutela previsti dal codice civile[73]. Come evidenziato sopra, tuttavia, è difficile immaginare che si riescano a prevedere e a codificare in anticipo tutte le possibili reazioni. D'altronde occorre rilevare come il ricorso agli organi giurisdizionali per ottenere l'esecuzione di uno smart contract possa rivelarsi estremamente complesso, a causa della lentezza di adeguamento del sistema alle nuove tecnologie. Per tale motivo, le parti ben potrebbero considerare di ricorrere ai sistemi di risoluzione alternativa delle controversie come l'arbitrato: strumento flessibile, che ben si adatta alle caratteristiche dei contratti intelligenti. All'interno del codice dello smart contract può essere inserita una clausola compromissoria che stabilisca che ogni eventuale controversia derivante dall'esecuzione del contratto stesso sia demandata alla competenza esclusiva di un arbitrato. Lo smart contract potrebbe attivare automaticamente il meccanismo di risoluzione della lite e potrebbe, a sua volta, utilizzare l'infrastruttura blockchain: la sentenza verrebbe registrata a sua volta nel *digitalized ledger* ed eseguita sulla stessa blockchain, tramite l'esecuzione di un codice che preveda il trasferimento delle somme riconosciute come dovute dal lodo arbitrale dal conto riconducibile alla parte condannata a quello riconducibile alla parte vincitrice.

[73] Per esempio, la clausola risolutiva espressa ex art. 1456 c.c., la sospensione dell'esecuzione in caso di mutamento delle condizioni patrimoniali di controparte ex art. 1461 c.c., il diritto di ritenzione previsto dagli artt. 2756 e 2761 c.c., il pegno irregolare art. 1851 c.c., ecc.

2.4 *Smart contract*: un approfondimento

Fino a qualche tempo fa, lo sviluppo delle tecnologie blockchain è avvenuto essenzialmente a prescindere da qualsiasi valutazione o considerazione circa la loro compatibilità con gli ordinamenti nazionali, ritenuti quasi degli avversari nei confronti di un nuovo sistema, caratterizzato dalla virtualità, dalla decentralizzazione (attraverso la quale si vogliono porre tutti i soggetti su di un piano di virtuale equivalenza), dall'indipendenza (intesa anche nel senso di alternatività o alterità rispetto ad ogni ordine precostituito) e dall'autogoverno (ogni vicenda che si svolge all'interno della blockchain è dominata dalla "legge" del codice informatico e del consenso distribuito). Mano a mano che il fenomeno è uscito dalla ristretta cerchia di *early adopter,* cui era originariamente confinato, estendendosi verso la generalità del pubblico e degli operatori economici, il contesto è gradualmente mutato. Da un lato, infatti, le tecnologie *DLT* hanno suscitato un interesse sempre crescente da parte delle autorità di regolamentazione e vigilanza, della letteratura scientifica e dei legislatori. Nonostante, in un primo momento, tale interesse si sia concentrato principalmente sulla materia delle criptomonete, in quanto essa costituisce la prima applicazione concreta della blockchain, successivamente si registrano i primi sporadici, ma significativi, interventi normativi anche con riferimento agli smart contract, sulla scorta del loro considerevole potenziale applicativo. Dall'altro lato, l'evoluzione delle *DLT* si mostra più sensibile e meno impermeabile alle sollecitazioni esterne.

La dottrina giuridica, specialmente di matrice anglosassone, ha da subito riservato una notevole attenzione al tema degli smart contract, interrogandosi su un possibile quadro definitorio, nonché sui connotati caratterizzanti ed essenziali di tali strumenti. Anche in assenza di una definizione universalmente condivisa, si ritiene opportuno evidenziare quella proposta da Christopher D. Clack, Vikram A. Bakshi e Lee Braine, che risulta particolarmente adeguata: *«a smart [legal] contract is an automatable and enforceable agreement. Automatable by computer, although some parts may require human input and control. Enforceable either by legal enforcement of rights and obligations or via tamper-proof execution of computer code»*. Tale definizione, ripresa ed approfondita nel contributo della Banca europea per la ricostruzione e lo sviluppo (EBRD), permette di chiarire la distinzione, ricorrente in letteratura che sussiste tra «*smart contract code*» e *«smart legal contract»*. La prima espressione si riferisce agli smart contract nella loro accezione meramente informatica e descrive un software, collocato all'interno di un sistema *DLT,* che utilizza la logica condizionale per determinare il verificarsi di una o più

condizioni prestabilite; a seguito di tale controllo, esso compie automaticamente una specifica operazione (secondo lo schema *if-then*), che può avere o meno rilevanza per il diritto. Il secondo termine, invece, indica un contratto (inteso nel suo significato giuridico) rappresentato, del tutto o in parte, attraverso un codice informatico, le cui prestazioni sono eseguite, parzialmente o totalmente, in via automatica da un programma per elaboratore inserito in una blockchain. È proprio il collegamento con le *DLT* a costituire il fattore maggiormente innovativo e interessante degli smart contract, in quanto consente di "saldare" il momento dell'accordo con la successiva fase dell'esecuzione del contratto *(«blockchains collapse agreement and execution. Because a smart contract both is the agreement and executes it»),* rimuovendo la distinzione tra queste due fasi contrattuali. L'ambizioso risultato che si intende conseguire è quello di rendere virtualmente impossibile non adempiere. Quindi, in questo modo, il pericolo che uno dei contraenti si renda inadempiente rispetto alle proprie obbligazioni non verrebbe semplicemente mitigato attraverso il deterrente costituito dai tradizionali rimedi previsti dall'ordinamento, ma, piuttosto, risulterebbe estinto alla radice.

L'idea di esprimere un rapporto contrattuale in forma elettronica non è certo nuova, così come non lo è quella di assegnare ad un software il compito di concorrere alla formazione della volontà negoziale, all'interpretazione o all'esecuzione dell'accordo.

Almeno a partire dal 1969, infatti, è stato avviato lo sviluppo di sistemi in grado di rappresentare e classificare gli elementi di un contratto in termini idonei ad essere elaborati da un programma informatico. Già allora, l'obiettivo che si intendeva conseguire non era il semplice trasferimento del testo di un accordo su di un documento elettronico, bensì la creazione di un modello che consentisse di raffigurare il contenuto di un contratto attraverso un linguaggio formale, comprensibile e processabile da un elaboratore, in luogo (o a fianco) dell'utilizzo del linguaggio naturale. Si cerca, cioè, di trasporre (ove possibile) la semantica contrattuale in chiave algoritmica: in questo senso, ad esempio, il concetto di «pagamento» può essere espresso con un'operazione che prevede il raffronto dei movimenti di denaro avvenuti tra due parti. L'aspetto forse più interessante di queste figure, definite alcuni decenni più tardi *data-oriented contract*,[74] è costituito dal fatto che una macchina diviene per la prima volta destinataria delle

[74] «A *"data-oriented" contract* is one in which the parties have expressed one or more terms or conditions of their agreement in a manner designed to be processable by a computer system. Typically, the parties express core elements as precisely defined computer data, rather than (or in addition to) a written language document to facilitate computer analysis, automation, or communication of their contractual obligations».

pattuizioni contenute nel contratto. La rappresentazione del contenuto contrattuale in termini informatici apre la strada all'ingresso dell'automazione. In altre parole, diviene possibile che sia lo stesso software ad intervenire dinamicamente in un rapporto negoziale, sulla base della combinazione tra un insieme di istruzioni predefinite ed una serie di input forniti al programma. Dunque, alla descrizione in forma algoritmica dell'accordo viene aggiunto il collegamento con le informazioni necessarie al software per interagire con il contratto (ad esempio, il programma deve essere anche capace di interloquire con un registro degli incassi e dei pagamenti per poter stabilire se il prezzo della merce è stato corrisposto entro il termine pattuito), allo scopo di consentire lo svolgimento in via automatizzata di determinate operazioni. Si parla, in simili ipotesi, di *computable contract*. L'applicazione delle logiche suddette ha portato, nel corso degli anni '70, alla nascita del modello *Electronic Data Interchange* (*EDI*), sviluppato per consentire lo scambio standardizzato di informazioni digitali tra operatori commerciali, e che risulta aver conseguito un buon successo in termini di prevenzione del contenzioso giudiziario.

Gli smart contract aggiungono, al quadro precedente, una novità fondamentale, costituita dalla loro particolare modalità di esecuzione delle prestazioni; mentre, in ultima istanza, l'adempimento di un *data-oriented contract* o di un *computable contract* può sempre essere interrotto o impedito mediante un'azione, anche unilaterale, posta in essere da uno dei contraenti, nel caso degli smart contract questa possibilità è esclusa *ab origine*. Nel momento in cui una transazione viene disposta all'interno di una blockchain essa è condivisa e replicata tra tutti i nodi che compongono la rete, uscendo così dalla sfera di intervento dei singoli utenti. Gli stessi meccanismi di consenso, che regolano automaticamente la tenuta del registro distribuito, vengono utilizzati per computare le operazioni e i trasferimenti stabiliti nello smart contract. Al verificarsi delle condizioni previste, ai fini della sua attuazione, la transazione diviene irrevocabile, irreversibile ed immutabile, sebbene non in modo del tutto assoluto. La realizzazione delle prestazioni dedotte nel contratto viene, così, svincolata dal fattore umano. Occorre, tuttavia, tenere presente che lo schema di attuazione automatica proprio degli smart contract è in grado di manifestare appieno la sua efficacia soltanto nell'ambito del contesto tecnologico delle *DLT*.

L'esecuzione degli smart contract , infatti, perde la caratteristica di essere effettiva e "resistente alle manomissioni"(*tamper proof*) quando nel trasferimento viene coinvolta

un’articolazione della realtà collocata al di fuori della blockchain: fino a quando lo scambio avviene tra entità o risorse che nascono ed esistono unicamente nel registro distribuito (come le criptovalute), il sistema si rivela efficace e potenzialmente autosufficiente; diversamente, se ad essere coinvolti sono beni o diritti non incorporati nella blockchain, gli smart contract non possono garantire la corretta ed effettiva esecuzione delle prestazioni in essi contenute.

2.5 Le problematiche dello strumento

La natura informatica, automatizzata e distribuita degli smart contract presenta, oltre ad interessanti profili applicativi, numerose problematiche che originano dalle loro caratteristiche tecniche. Innanzitutto, va considerata la questione del linguaggio. Il linguaggio umano, infatti, viene sostituito dal codice di programmazione, che rimpiazza la normale comprensibilità, flessibilità e duttilità del linguaggio naturale con la rigida dialettica binaria tra 0 e 1. Se, da un lato, il linguaggio informatico consente di comporre un regolamento contrattuale che sia privo delle incertezze e delle ambiguità proprie del linguaggio dell’uomo, in quanto il contratto viene strutturato secondo lo schema ‘se X allora Y’, all’interno del quale le variabili e le condizioni possiedono un solo ed unico significato oggettivo (che, però, non necessariamente coincide con l’intenzione delle parti), dall’altro lato, l’utilizzo del codice pone dei dubbi in ordine alla intelligibilità dell’accordo da parte dei contraenti e, conseguentemente, alla validità del consenso da essi prestato, specie se sono sprovvisti di particolari competenze in campo informatico e/o appartengono a categorie tutelate. In particolare, ci si chiede se nel concetto di “libertà di lingua”, con il quale si intende la generale libertà dei soggetti privati di scegliere ed impiegare una qualsiasi lingua nello svolgimento della propria negoziale, possa essere ricompresa anche la facoltà di adottare il codice informatico come “lingua” del contratto, e quali siano i presupposti per l’applicazione della disciplina dei vizi della volontà nell’eventualità di una inesatta rappresentazione del contenuto dell’accordo dovuta all’uso del linguaggio di programmazione. Un possibile metodo, per superare questo genere di problematiche, è stato rinvenuto nell’idea di connettere, direttamente allo smart contract, un documento contrattuale elettronico, redatto in linguaggio umano, che ne rappresenti e costituisca l’esplicitazione. Il sistema, denominato anche *ricardian smart*

contract, si compone di tre elementi collegati tra loro: il testo del contratto (che rende direttamente comprensibile il codice informatico), lo smart contract ed i parametri che influenzano e determinano la sua esecuzione.

La trasposizione del linguaggio e delle regole del diritto in forma algoritmica rappresenta una tematica di notevole attrattiva, ma non priva di difficoltà. Fin dall'inizio degli anni '60, la scienza giuridica ha cominciato ad avvertire le potenzialità connesse all'utilizzo degli elaboratori e della logica matematica.

Tra i primi esperimenti applicativi in materia, può essere rammentata la "traduzione" del *British Nationality A*ct del 1981 nel linguaggio di programmazione *Prolog*, acronimo per *Programming in Logic*. L'obiettivo del lavoro era costituito dallo studio del procedimento di formalizzazione informatica di un testo normativo e del ragionamento giuridico sottostante, nella convinzione che una simile indagine avrebbe favorito sia lo sviluppo delle tecnologie connesse all'intelligenza artificiale (in relazione alle quali il diritto costituisce un ottimo riscontro per i linguaggi formali di rappresentazione della conoscenza e per gli schemi di risoluzione dei problemi), sia l'intelligibilità di una legge, il *British Nationality Act* appunto, piuttosto articolata e controversa.

Tra la fine del secolo scorso e l'inizio del nuovo, il filone di ricerca tra scienza informatica e diritto ha affrontato nello specifico, la questione relativa alla formalizzazione dei contratti in un linguaggio informatico che fosse capace di riprodurre il contenuto dell'accordo quanto più fedelmente possibile, e che consentisse l'automazione della stesura, dell'analisi, della revisione e dell'esecuzione dei rapporti contrattuali. Il fine di questa indagine, oltre a costituire la base sulla quale sono fondati gli smart contract , ha portato, parallelamente, alla nascita di una serie di soluzioni software incentrate sull'automazione della redazione di nuovi contratti (ausilio alla stesura di documenti giuridici attraverso l'utilizzo del linguaggio simbolico e della formalizzazione informatica), e sull'analisi di quelli già esistenti (come nel caso dell'impiego delle tecnologie di apprendimento automatico, il c.d. *machine learning*, per segnalare la presenza, all'interno del testo di un accordo, di eventuali incoerenze, ambiguità e altri fattori di rischio sul piano logico o lessicale). Con particolare riferimento all'ambito accademico, merita senz'altro di essere segnalata l'attività svolta dallo *Stanford Center for Legal Informatics (Codex)*, relativa soprattutto allo studio della *computational law*: branca dell'informatica del diritto che si occupa della meccanizzazione dell'analisi giuridica, foriera di importanti riflessi applicativi. Tra le osservazioni più interessanti

emerse dal settore di indagine costituito dalla *computational law* vi è la considerazione che trasporre un contratto in linguaggio informatico importa la possibilità di sottoporlo ad un procedimento di verifica formale. Questa tecnica, ideata per l'esame teorico dei sistemi hardware e software, al fine di far emergere eventuali anomalie di funzionamento, consente di dimostrare o contestare in via matematico-formale la rispondenza di un determinato strumento, ad esempio un programma per elaboratore, a specifici requisiti o caratteristiche. Sottoporre un contratto a verifica formale potrebbe, quindi, permettere di stabilire se le pattuizioni in esso contenute sono logicamente compatibili le une con le altre e se determinano, nel complesso, un assetto di interessi effettivamente coincidente con quanto voluto dalle parti. Per raggiungere tale risultato si è proposto di utilizzare il *model checking*, metodo di verifica formale che si caratterizza per essere facilmente automatizzabile, consistente nell'esplorazione sistematica ed esaustiva del modello matematico che rappresenta il sistema hardware o software da sottoporre a test (in questo caso il contratto). Allo stesso tempo, tuttavia, esprimere un contratto in forma algoritmica comporta l'introduzione di un nuovo insieme di criticità, che consistono nell'eventualità che il codice informatico illustrante l'accordo sia affetto da errori, difetti o vulnerabilità, causati ad esempio da errori di sintassi nel codice, che possono portare il programma ad un'inesatta interpretazione dei requisiti necessari per effettuare una determinata azione, o che possono dare agli utenti (le parti del contratto) la possibilità di porre in essere comportamenti illegittimi. A tal proposito, il riferimento forse più significativo riguarda il caso *The DAO*, una piattaforma partecipativa per la raccolta di capitale di rischio, costituita attraverso uno smart contract collocato sulla blockchain ethereum. Con l'acronimo *DAO* si identifica la categoria delle *Decentralized Autonomous Organizations*: entità che risiedono su di un registro distribuito, le cui attività sono svolte in parte autonomamente dal software e in parte mediante l'apporto, riservato soprattutto alle questioni decisionali, di soggetti umani. Nel maggio del 2016, alcuni componenti della comunità blockchain hanno utilizzato le possibilità tecniche offerte da ethereum per realizzare una *Decentralized Autonomous Organization*, denominata «*The DAO*», con lo scopo di raccogliere fondi, in forma di criptomoneta, da destinarsi al finanziamento di attività sia commerciali che senza scopo di lucro. Tuttavia, ad appena un mese di distanza dal lancio della piattaforma, che in questo breve lasso di tempo aveva ricevuto un ammontare di criptovaluta per un valore superiore ai 150 milioni di dollari, uno dei partecipanti, sfruttando una vulnerabilità del codice informatico impiegato per realizzare lo smart contract sul quale poggiava *The DAO*, è riuscito ad appropriarsi indebitamente

di più di un terzo dei fondi, determinando, alla fine dei conti, il fallimento di tutta l'iniziativa. La vicenda, come pure le misure che sono state adottate nel tentativo di mitigarne gli effetti più negativi, offre alcuni fondamentali spunti di riflessione.

Si è detto che i trasferimenti stabiliti in uno smart contract sono irrevocabili, irreversibili e immutabili, in quanto vengono eseguiti dal sistema in via automatica al verificarsi delle condizioni previste dallo stesso smart contract, senza che alcun intervento umano possa impedirli o modificarli. Proprio in ragione di questa mancanza di flessibilità, risulta di importanza primaria che il codice informatico alla base dello smart contract sia, da un lato, esente da anomalie o vulnerabilità e, dall'altro, in grado di rappresentare fedelmente l'assetto di interessi che le parti intendono effettivamente realizzare. In proposito, alcuni autori hanno suggerito di utilizzare le tecniche della verifica formale anche con riferimento agli smart contract, ritenendo che tali procedimenti siano in grado di prevenire il ripetersi di eventi analoghi al caso *The DAO*. Allo stesso tempo, però, occorre rilevare come gli stessi caratteri dell'irrevocabilità, dell'irreversibilità e dell'immutabilità non siano del tutto assoluti. La regola fondamentale che governa la blockchain (e quindi, di riflesso, anche gli smart contract) è quella del consenso distribuito; essa funge da presidio e garanzia della *trustless trust* sulla quale si fondano tali sistemi. Detta regola, tuttavia, presenta anche un lato negativo: infatti, almeno in linea teorica, consente di modificare o cancellare una transazione già effettuata sulla blockchain, a condizione che detto intervento incontri l'approvazione di un numero di partecipanti al sistema, capace di esprimere la maggioranza ai sensi del meccanismo di consenso distribuito utilizzato.

Per quanto riguarda le architetture blockchain basate su algoritmi di consenso di tipo *Proof-of-Work* (ad oggi ancora il più diffuso), il concetto di maggioranza è determinato non per teste, ma in relazione alla quota di potenza elaborativa immessa da ciascun soggetto nel sistema. È questa la strada che, non senza notevoli resistenze e soltanto a seguito di un lungo dibattito, si è scelto di percorrere con riferimento alla vicenda *The DAO*. La maggioranza dei partecipanti alla blockchain ethereum, riscontrata l'insufficienza e l'impraticabilità tecnica di interventi meno invasivi, si è accordata per "riscrivere" il registro delle transazioni, eliminando l'operazione con la quale era stata distratta una parte dei fondi raccolti da *The DAO* e ripristinando lo *status quo ante*. La decisione, del tutto estrema ed eccezionale, ha suscitato numerose critiche, dovute soprattutto alla considerazione che in tal modo si è deliberatamente sacrificato il principio, da molti ritenuto imprescindibile, della certezza ed immodificabilità delle

transazioni, provocando un'inevitabile crisi di fiducia. L'esperienza di *The DAO* rappresenta un efficace esempio della rigidità che connota gli smart contract. La sussistenza di un errore di programmazione, la presenza di una vulnerabilità informatica o anche il semplice verificarsi di una circostanza non prevista possono determinare esiti quasi irreversibili, in considerazione della notevolissima difficoltà e del prezzo (in termini di perdita di credibilità) che una riscrittura delle transazioni contenute nella blockchain comporta per l'intero sistema. Dunque, in concreto, gli unici interventi che le parti possono operare su di uno smart contract, già formalizzato, rischiano di essere (soltanto) quelli già esplicitamente contemplati, *ab origine*, nell'accordo stesso, con l'inevitabile conseguenza, specialmente con riferimento ai rapporti contrattuali più complessi, di un notevole incremento dei costi negoziali o, addirittura, della sostanziale impossibilità di ricorrere ad uno smart contract. Le parti, infatti, devono regolare preventivamente e specificatamente tutte le circostanze che possono astrattamente verificarsi: perciò, in ipotesi di accordi non facilmente standardizzabili, i contraenti potrebbero trovarsi a dover sopportare costi ed oneri molto superiori rispetto a quelli che avrebbero sostenuto optando per un contratto tradizionale. Sempre ragionando in questa prospettiva, non si può fare a meno di rilevare come l'inflessibilità degli smart contract incida profondamente anche sull'applicabilità delle regole e dei rimedi previsti dall'ordinamento in relazione alle diverse forme di patologia del contratto. L'automaticità dell'esecuzione, unita con la non modificabilità delle transazioni, comporta, ad esempio, il pericolo che gli effetti di una eventuale sentenza di nullità o annullamento restino puramente teorici, in quanto le prestazioni contenute nello smart contract verranno comunque eseguite dal sistema, dal momento che, anche in presenza di un contratto invalido, la possibilità di non adempiere resta esclusa in radice. In termini diversi, si può affermare che gli smart contract realizzano un'inversione del paradigma tradizionale del diritto contrattuale: «*from ex post authoritative judgment to ex ante automated assessments*». Resta, tuttavia, il problema di contemperare le rigidità di un meccanismo concepito *«[to] eliminate the act of remediation, by admitting no possibility to breach»*, che trasla e comprime tutte le possibilità di intervento sul contratto nel momento della stipula, con la necessità di assicurare un efficace controllo giudiziario a posteriori. Detto bilanciamento è ineliminabile: sarebbe, infatti, impensabile rinunciare alle tutele e alle garanzie offerte dall'ordinamento in nome di un'autonomia negoziale assoluta ed illimitata. Sarebbe, inoltre, vano pensare, come dimostra il caso *The DAO*, che le parti possano sempre essere in grado di regolare a priori tutti gli elementi capaci di incidere sul proprio rapporto

contrattuale, siano essi relativi a difetti, o vulnerabilità del codice informatico, o dovuti, più in generale, al verificarsi dell'imprevisto o dell'imprevedibile.

Questo rovesciamento di prospettive comporta, sempre restando nell'esempio di un contratto dichiarato nullo o annullato, una notevole difficoltà nel ristabilire lo *status quo ante*, data l'inalterabilità dei sistemi blockchain ad ogni intervento di modifica del registro delle transazioni. Ciò determina il rischio che non sia possibile riportare la sfera giuridica delle parti nella situazione in cui si sarebbe trovata se lo smart contract non fosse stato mai concluso. Infatti, sebbene possano certamente ipotizzarsi rimedi di tipo restitutorio o risarcitorio (come l'obbligo di concludere un nuovo smart contract che inverta i trasferimenti effettuati dal precedente), gli effetti restano, comunque, profondamente differenti nella sostanza: una cosa è rifiutarsi di eseguire un contratto invalido, altra è chiedere (ed ottenere) la ripetizione di quanto già prestato. Basti soltanto pensare al caso in cui un bene trasferito in esecuzione di uno smart contract revocato sia già stato ritrasferito, con un successivo smart contract, a terzi. Conciliare adeguatamente le esigenze della certezza ed immodificabilità delle transazioni blockchain con il necessario rispetto delle garanzie e delle forme di tutela prescritte dagli ordinamenti giuridici rappresenta una delle prove più impegnative alle quali è chiamato a rispondere anche (e forse soprattutto) il legislatore. Sotto un ulteriore profilo, l'ambiguità del codice informatico rende notevolmente complessa l'inserzione, in uno smart contract, di clausole contrattuali o espressioni volutamente dubbie o vaghe, cui le parti possono voler ricorrere qualora non siano in grado di predeterminare esattamente il contenuto delle reciproche prestazioni. Infatti, nel caso in cui il rapporto negoziale richieda un certo livello di astrazione o di flessibilità nel valutare situazioni esterne, oppure la successiva condotta dei contraenti, potrebbe risultare impossibile, o semplicemente troppo impegnativo, traslare simili variabili in espressioni stimabili da un programma informatico.

CAPITOLO III

SMART CONTRACT E BLOCKCHAIN: LEGISLAZIONI INTERNAZIONALI A CONFRONTO

3.1 Premessa

Il fenomeno Blockchain è sempre più al centro dell'attenzione delle istituzioni sul piano giuridico e normativo e rappresenta certamente il paradigma dell'evoluzione attuale di Internet nel processo di sviluppo delle tecnologie digitali.

L'Italia con il DL Semplificazioni[75] fa certo avanguardia nella normativa blockchain, ma si pone anche all'interno di un percorso internazionale.

Per tale ragione, risulta interessante individuare i modelli di regolamentazione del fenomeno, facendo riferimento alle principali iniziative esistenti nel panorama globale.

Ma in un contesto ancora incerto e contraddittorio, ad oggi sono pochi i Paesi che si sono spinti nella regolamentazione giuridica degli smart contract[76]. In alcuni Stati americani

[75] Il decreto Semplificazioni 2019 introduce la definizione normativa delle tecnologie basate su registri distribuiti (blockchain) e degli smart contract. Il decreto prevede, inoltre, che la memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produca gli effetti giuridici della validazione temporale elettronica. L'identificazione di un preciso inquadramento giuridico, unitamente alle disposizioni europee in materia di antiriciclaggio e alle relazioni pubblicate da Banca d'Italia, favorisce la generale accettazione delle criptoattività e lo sviluppo di nuove attività d'impresa.

[76] Il legislatore italiano, tra i primi in Europa, è intervenuto con il Decreto Semplificazioni 2019 per dare una prima regolamentazione al fenomeno degli Smart Contract e della blockchain.
L'idea di un contratto intelligente, pur risalendo alla metà degli anni '70, ha trovato solo nella blockchain la tecnologia perfetta per darne reale attuazione. Il concetto di fiducia, posto come visto alla base dell'infrastruttura blockchain, risulta perfettamente adattabile a tale forma contrattuale. Con Smart Contract si indica la traduzione in codice di un contratto in modo tale da eseguire automaticamente le clausole contrattuali al verificarsi, sempre in modo automatico, di determinate condizioni stabilite ex ante e inserite all'interno del codice. Il contributo umano, dunque, è tale solamente per quanto attiene alla fase di progettazione del codice in quanto una volta realizzato le azioni successive si concretano in modo automatico. Al realizzarsi di predeterminati input, il codice fa corrispondere predeterminati output. Fondamentale risulta dunque essere una dettagliata descrizione iniziale delle plurime ipotesi contenute nel contratto. In tal senso vi sarà sempre più la necessità di un lavoro congiunto tra esperti legali ed esperti del settore informatico. I vantaggi di un contratto intelligente sono relativi in primis ad un risparmio di tempo e costi, oltre che di una certezza di giudizio relativamente ad un contratto che non risulta essere interpretabile. L'obiettivo è proprio quello di eliminare (per quanto attiene alle fasi successiva alla progettazione del contratto) eventuali intermediari e sostituirli con un sistema il più certo ed oggettivo possibile. Quest'ultimo punto rappresenta però anche uno possibile svantaggio. Come detto sopra, sarà fondamentale un preciso lavoro in fase di creazione del codice al fine di determinare in modo immodificabile la volontà delle parti che dovranno poi attenersi completamente a quanto pattuito in fase di progettazione. Serviranno poi delle regole ben precise volte a regolamentare eventuali atipicità. Altra

come l'Arizona, il Tennessee, l'Ohio e il Nevada sono state emanate delle legislazioni o delle proposte di legge che ne riconoscono già valore. Mentre altri Stati come la California e lo Stato di New York hanno posto in essere delle task force che sono volte principalmente allo studio degli impatti e delle possibilità applicative.

In Europa, il regolatore si è accorto dell'importanza di definire a livello giuridico la validità di uno smart contract, quindi ha avviato dei processi di valutazione che non si sono ancora conclusi. Anche il Parlamento europeo è intervenuto chiedendo alla Commissione europea di legiferare in tema Blockchain e di porre in essere un'attenta analisi di costi e benefici degli smart contract.

Pur essendo senza dubbio una tecnologia dalle prospettive interessanti, la Blockchain, pertanto, può essere ancora definita di frontiera, con un numero limitato di casi applicativi e diverse incertezze sul quadro legislativo di contorno. C'è una particolare area della Blockchain che è in uno stadio ancora più sperimentale: quella degli Smart Contract.

Affinché uno Smart Contract funzioni è indispensabile il consenso tra le parti. Ma nonostante tutta la fiducia possibile tra gli interlocutori, per il regolare funzionamento degli Smart Contract risulta indispensabile la presenza di un intermediario che ne garantisca l'affidabilità e impedisca possibili manomissioni. L'alternativa è rappresentata dall'inserimento, quindi, di una procedura automatizzata che si sostituisca a questo intermediario, garantendo l'immutabilità e l'affidabilità degli Smart Contract. Questa funzione può oggi essere assolta dall'applicazione della tecnologia Blockchain.

Dunque, al di fuori del territorio nazionale, gli interventi più significativi in materia sono stati adottati soprattutto da alcuni paesi tecnologicamente all'avanguardia nel contesto asiatico. Capofila in tal senso sono stati gli Emirati Arabi e la Cina. Anche nel panorama normativo statunitense nel corso del 2018 si è registrato un numero crescente di interventi legislativi statali volti a regolamentare la tecnologia Blockchain.

In ambito UE, il Parlamento Europeo con la Risoluzione del 3 ottobre 2018 ha riconosciuto la rilevanza della tecnologia Blockchain e ha auspicato l'adeguamento del quadro giuridico-normativo vigente a tali innovazioni mediante la definizione di strategie

---

tematica rilevante attiene alla necessità di individuare chi abbia la possibilità e di conseguenza la responsabilità, di garantire l'esattezza degli input immessi nel codice. In tal senso sarebbe auspicabile individuare soggetti terzi che siano in grado di fornire determinate garanzie tecniche.

Tale nuova forma di contratto dovrà considerare, nel nostro ordinamento, in primo luogo gli artt. 1321-1469 del codice civile. Dovrà necessariamente contenere gli elementi di cui all'articolo 1325 c.c. ossia l'accordo tra le parti, la causa, l'oggetto e la forma quando prevista. Particolare problematica è quella che attiene alla possibilità di riconoscere, qualora sia imprescindibile, la forma scritta allo Smart Contract.

finalizzate ad incrementare il livello delle competenze digitali e favorire la diffusione generalizzata di tale tecnologia.

3.2 L'orientamento dell'Unione europea

Nell'ambito dell'Unione europea, a seguito di una serie di iniziative promosse dalla Commissione europea *("Blockchain4EU*: *Blockchain per le trasformazioni industriali", "Osservatorio e forum dell'UE sulla blockchain", "Blockchain per il bene sociale", "Studio sull'opportunità e sulla fattibilità di una struttura blockchain dell'UE"),* il Parlamento europeo con la Risoluzione del 3 ottobre *"sulle tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione",* ha riconosciuto la rilevanza della tecnologia Blockchain come strumento «*che può democratizzare i dati e rafforzare la fiducia e la trasparenza»*, in quanto «*rafforza l'autonomia dei cittadini»* e migliora «*l'efficienza dei costi delle transazioni eliminando intermediari e costi di intermediazione, oltre ad aumentare la trasparenza delle transazioni»*.
A tal fine, viene auspicato l'adeguamento del quadro giuridico-normativo vigente a tali innovazioni, per assicurare la "certezza del diritto" e "il rispetto del principio della neutralità tecnologica", mediante la definizione di strategie finalizzate ad incrementare il livello delle competenze digitali e favorire la diffusione generalizzata di tale tecnologia.

3.2.1 Italia

Il legislatore italiano, tra i primi in Europa, è intervenuto con il Decreto Semplificazioni, convertito in legge a febbraio 2019, per dare una prima regolamentazione agli Smart-Contract e alla blockchain, assegnando, quindi, validità giuridica.

In particolare l'art. 8-ter della legge[77] al primo comma definisce come tecnologie basate su registri distribuiti (*DLT - Distributed Ledgers Technology*) quelle tecnologie e quei

[77] L'articolo 8-ter del Decreto Semplificazioni fornisce un primo inquadramento giuridico della blockchain e degli Smart Contract nel nostro ordinamento. Tali definizioni si aggiungono alle disposizioni UE in tema di antiriciclaggio e alle relazioni della Banca d'Italia che avevano già riconosciuto formalmente, nei rispettivi ambiti, il fenomeno delle criptoattività basate sulla blockchain. Nello specifico, il summenzionato articolo fa riferimento alle Tecnologie basate su registri distribuiti e Smart Contract. Con il primo termine

protocolli informatici *"che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili".*

Il secondo comma definisce come smart contract *"un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse. Gli smart contract soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con linee guida da adottare entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto".*

Il terzo comma stabilisce poi *che "la memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui all'articolo 41 del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014".* Questo Regolamento Ue è il cosiddetto Regolamento "eIDAS" *o "electronic IDentification Authentication and Signature,* che stabilisce le condizioni per il riconoscimento reciproco in ambito di identificazione elettronica e le regole comuni per le firme elettroniche, l'autenticazione web e i relativi servizi fiduciari per le transazioni elettroniche. In sostanza, dice ora la legge, la certificazione tramite blockchain ha un valore giuridico alla stessa stregua di quello assegnato ai "dati che in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi

si individua di fatto la blockchain, definendo la stessa come quella "tecnologia che utilizza un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tale da consentire la registrazione, la convalida, l'aggiornamento, l'archiviazione di dati (sia in chiaro che ulteriormente protetti da crittografia) verificabili da ciascun partecipante, non alterabili e non modificabili". Lo Smart Contract invece viene definito dal legislatore come quel "programma per elaboratore che opera su tecnologie basate su registri distribuiti la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse".
Dunque, il legislatore italiano, attento alla problematica attinente al requisito della forma scritta, afferma che "gli Smart Contract soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia Digitale (AgID) con linee guida da adottarsi entro 90 giorni dall'entrata in vigore della legge di conversione del decreto". Ruolo fondamentale sarà dunque assunto da questa Agenzia, la quale dovrà stabilire con assoluta precisione i caratteri che deve avere il codice alla base dello Smart Contract. Solo il rispetto di tali caratteri contenuti nelle future linee guida permetterà al contratto intelligente di integrare il requisito della forma scritta.

esistevano in quel momento" (questa è la definizione che il Regolamento assegna al concetto di "validazione temporale elettronica").[78]

Di fatto questo comma rappresenta la base per far sì che qualunque controparte di una blockchain aperta possa giuridicamente far valere nei confronti di terzi quanto certificato dalla blockchain, senza quindi che sia necessario preventivamente firmare un contratto privato con gli altri aderenti alla blockchain, come avviene nel caso delle blockchain private (per esempio quelle create dalle grandi banche internazionali).

Infine, il quarto comma dell'art.8-ter della legge stabilisce che entro 90 giorni dalla data di entrata in vigore della legge, l'Agenzia per l'Italia digitale individui gli standard tecnici che le tecnologie basate su registri distribuiti debbono possedere perché possano essere riconosciute giuridicamente.

3.3 Gli interventi di regolamentazione negli Stati Uniti

Nel panorama normativo statunitense, è possibile focalizzare un crescente numero di interventi legislativi statali dedicata alla regolamentazione della tecnologia Blockchain. Si riporta:

-l'House Bill 2602, adottato il 12 aprile 2018 modifica lo statuto dello Stato dell'Arizona, al fine di formalizzare il divieto di introdurre regolamentazioni locali in materia di Blockchain, dirette a impedire e/o limitare agli individui la gestione delle transazioni mediante tecnologia Blockchain, costituente oggetto di esclusiva regolamentazione statale.

-Lo Stato della California con il Disegno di Legge n. 838 approvato 28 settembre 2018, dopo aver definito le caratteristiche essenziali della tecnologia Blockchain, autorizza le società per azioni che non emettono titoli in circolazione quotati in borsa a inserire nel

[78] Il Decreto Semplificazioni, oltre a fornire una prima definizione di blockchain e Smart Contract, evidenzia come "l'utilizzo di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui all'art. 41 del Regolamento UE n. 910/2014". Il c.d. Regolamento eIDAS, all'art. 41, evidenzia come alla validazione temporale elettronica debbano essere riconosciuti gli effetti giuridici e l'ammissibilità come prova in giudizio. La validazione temporale elettronica rilasciata in uno stato membro poi, è riconosciuta in tutti gli stati membri. La novità del Decreto Semplificazioni è particolarmente rilevante nel momento in cui la registrazione di un documento nella blockchain permette ora di garantire la certezza circa gli estremi temporali del documento stesso con la possibilità di opporre il tutto a terzi.

proprio atto costitutivo specifiche disposizioni che consentano la registrazione delle operazioni di emissione, trasferimento e conservazione effettuate dai propri azionisti mediante tecnologia Blockchain.

- Nello Stato del Connecticut, il Disegno di Legge n. 443 del 6 giugno 2018 ha istituito un gruppo di lavoro con il compito di formulare raccomandazioni funzionali a sviluppare un piano generale per favorire la crescita dell'industria Blockchain, mentre il Disegno di Legge n. 513 del 17 aprile 2018, ha previsto la costituzione del gruppo di lavoro preposto all'analisi dell'impatto della moneta digitale nella crescita economica delle imprese, anche al fine di incentivare l'utilizzo dello strumento degli Smart Contracts.

-Dello stesso contenuto il Disegno di Legge n. 3613 presentato il 12 marzo 2018 dello Stato del New Jersey, con cui si stabilisce la creazione della New Jersey Blockchain Initiative Task Force, con il compito di individuare i vantaggi derivanti dall'uso della tecnologia Blockchain nelle operazioni di conservazione dei registri e di erogazione di servizi, mediante lo sviluppo di database distribuiti protetti da algoritmi crittografici, al pari, altresì, di quanto previsto dal Disegno di Legge n. 8793 approvato dallo Stato di New York.

-Il Disegno di Legge n. 765 dello Stato di Vermont prevede l'implementazione di strategie in materia di Blockchain, al fine di promuovere l'efficienza degli apparati amministrativi e la produttività dei processi aziendali sia nel settore pubblica sia nel settore privato.

3.4 La legislazione nel contesto asiatico

Nel contesto asiatico è possibile focalizzare gli interventi più significativi in materia, adottati da alcuni Paesi tecnologicamente all'avanguardia, la cui strategia prioritaria mira alla valorizzazione della Blockchain come strumento fondamentale per migliorare le condizioni di vita dei cittadini, i servizi pubblici e qualsiasi altro aspetto della società e dell'economia.

Il modello di blockchain degli Emirati Arabi

Emblematico è il documento *"UAE Strategy for Artificial Intelligence (AI) 2031"* predisposto nell'ottobre 2017 dal governo degli Emirati Arabi Uniti, nella parte in cui viene delineato un nuovo modello di "Smart Government", basato sulla tecnologia Blockchain utilizzata per implementare l'efficienza e la qualità dei servizi pubblici erogati, grazie ad una significativa riduzione delle risorse sprecate a causa dei costi di transazione tradizionalmente previsti in tutti i settori e livelli governativi.

Tenuto conto delle coordinate generali definite nell'ambito del citato piano d'azione, è stata adottata la *"Dubai Blockchain Strategy",* con l'obiettivo di rendere *Dubai "la città più felice della Terra",* grazie all'utilizzo diffuso dell'Intelligenza Artificiale e della tecnologia Blockchain, in grado di garantire maggiori opportunità economiche, nonché la creazione di nuove industrie innovative e una più elevata efficienza governativa, nella prospettiva di rendere Dubai leader mondiale nel settore tecnologico entro il 2020, grazie al rilevante risparmio calcolato nella misura di 5,5 miliardi di dirham derivante dalla concreta attuazione della strategia operativa prevista.

Particolarmente interessanti risultano, altresì, gli interventi realizzati dal Governo cinese che, nell'ambito della strategia "Made in China 2025", diretta alla modernizzazione del settore industriale, incentiva in maniera particolarmente significativa il ricorso alla tecnologia IoT ("Internet delle Cose") e all'Intelligenza Artificiale, come strumenti fondamentali da utilizzare nella produzione di beni e servizi imprenditoriali.

A tal fine, dopo l'approvazione *del "Three-Year Guidance for Internet Plus Artificial Intelligence Plan (2016-2018)"* e del "*Three-Year Action Plan for Promoting Development of a New Generation Artificial Intelligence Industry (2018-2020)*", nel luglio 2017, il Consiglio di Stato cinese ha pubblicato il "*New Generation Artificial Intelligence Development Plan"*, finalizzato a sviluppare, grazie ad ingenti investimenti pubblici che prevedono l'erogazione di un importo complessivo pari a 150 miliardi di dollari, un piano strategico nazionale di Intelligenza Artificiale per rendere la Cina la principale potenza mondiale nel settore IA entro il 2030, affidando al Ministero della Scienza e della Tecnologia (MOST), il compito di coordinare e attuare i progetti di Intelligenza Artificiale e lo sviluppo della tecnologia Blockchain.

Inoltre, il Partito di governo ha pubblicato un documento divulgativo recante linee guida operative, dal titolo "Blockchain—Leading Cadre's Reader", per aiutare i rappresentanti istituzionali e i quadri dirigenti a comprendere il funzionamento della Blockchain, in

modo da condividere una visione strategica diffusa in grado di sfruttare le opportunità offerte dall'implementazione di sistemi basati su tale tecnologia.

Sul piano giurisprudenziale, proprio in Cina si registra un' interessante pronuncia che riconosce la rilevanza della Blockchain: la Corte Suprema, infatti, in un recente caso deciso nel settembre 2018 ha sancito il valore legale vincolante nelle controversie giudiziarie delle prove autenticate con tecnologia Blockchain, affermando testualmente che «*I tribunali riconosceranno i dati digitali presentati come prove se le parti interessate hanno raccolto e archiviato questi dati tramite blockchain con firme digitali affidabili o tramite una piattaforma di deposizione digitale che possa dimostrare l'autenticità di tale tecnologia utilizzata*».

3.5 Repubblica di San Marino

È interessante citare il caso di San Marino che ha emanato il "Decreto Delegato Blockchain". Questo atto, oltre a regolamentare l'emissione e la commercializzazione di token, ne disciplina anche il regime fiscale: tutti i ricavi delle operazioni effettuate con i token saranno esentasse nel territorio della Repubblica, mentre saranno soggetti a tassazione del Paese di destinazione. Tramite l'applicazione di questa normativa il governo di San Marino spera di trasformare il Paese in un importante centro tecnologico e di attrarre investimenti e start-up.

Dunque, la Repubblica di San Marino ha presentato, il primo marzo 2019 a San Marino il nuovo *Decreto Delegato Blockchain*, per garantire maggiore trasparenza, chiarezza e semplicità sulle norme per le applicazioni della Tecnologia del Registro Distribuito (*Distributed Ledger Technology*), con l'obiettivo di rilanciare l'economia del Paese all'insegna dell'innovazione e qualificarne e valorizzarne sempre più il profilo di *hub* tecnologico a livello mondiale.

Infatti, dallo studio del panorama normativo e regolatorio estero, è emersa l'esigenza di redigere una regolamentazione per disciplinare le applicazioni della tecnologia blockchain, con la finalità di creare un ecosistema, nel quale sia possibile operare grazie a norme chiare, precise e ben comprensibili. Lo scopo principale è quello di attrarre progetti basati su tecnologia blockchain dal respiro internazionale e posizionare la

Repubblica di San Marino come uno dei centri di eccellenza a livello mondiale, nonché come il miglior partner legislativo degli innovatori.

Il *Decreto Delegato Blockchain*, oltre a riconoscere la tecnologia blockchain con una definizione chiara e semplice, disciplina l'emissione di due categorie di strumenti digitali (*token)* quali paradigma di nuovi modelli economici: i *token* di utilizzo (che consentono l'accesso futuro ai prodotti e servizi offerti da un'azienda e, pertanto, non costituiscono un investimento né soggiacciono alle regole proprie delle attività di investimento) e i *token* di investimento (*security token,* strumenti digitali il cui valore deriva da un *asset* sottostante - azioni, strumenti finanziari partecipativi e titoli di debito dell'emittente - che può essere scambiato).

Tuttavia, in questo primo stadio la nuova disposizione non regolamenta le cosiddette "criptovalute" (token di pagamento o payment token), che rappresentano una parte residuale del mercato di riferimento e che non possono prescindere dalle regole del mercato monetario e dei servizi di pagamento.

I maggiori punti di forza della normativa della Repubblica di San Marino rispetto agli altri Paesi sono, da una parte, il Decreto Delegato che diviene uno strumento fondamentale per consentire un pronto adeguamento di pari passo con gli avanzamenti della tecnologia, dall'altra le funzioni regolamentari in capo a *San Marino Innovation*[79] al fine di realizzare il *"modello sandbox",* la cui caratteristica è di avere un perimetro ben delineato e solido e da confini non alterabili, al cui interno gli operatori possono muoversi in maniera scorrevole, ma non in assenza totale di regole nei loro movimenti.

Dunque, secondo il Decreto, nel momento in cui un Ente Blockchain, soggetto giuridico che ha ottenuto un particolare riconoscimento da parte di San Marino Innovation, emetterà strumenti digitali (token) per farli acquistare dagli utenti (la cosiddetta ITO, Initial Token Offering ovvero Offerta Iniziale di Token) dovrà sottostare a specifiche regole.

[79] Il Decreto Blockchain rappresenta un tassello fondamentale di un percorso già intrapreso con il Decreto Innovazione, specificamente rivolto alle imprese ad alto contenuto tecnologico, sia start-up che grandi aziende, anch'esso frutto della collaborazione con *San Marino Innovation*, e che proseguirà con altre iniziative".
San Marino ha scelto un percorso misto di norme di legge e competenze di enti regolatori: è stato scelto il decreto delegato come strumento fondamentale per consentire un pronto adeguamento di pari passo con gli avanzamenti della tecnologia e, al contempo, sono state individuate diverse funzioni regolamentari in capo a *San Marino Innovation*.

San Marino Innovation avrà quindi il potere di condizionare l'offerta grazie a una serie di misure rafforzate a tutela dell'utente e del mercato. L'Istituto potrà richiedere un'integrazione delle informazioni fornite dall'Ente Blockchain, al fine di preservare la trasparenza e la credibilità del sistema, così come proibire o sospendere l'offerta/pubblicità in caso di violazione delle disposizioni di legge.

Una caratteristica della proposta sammarinese rispetto a tutte le altre esistenti è poi l'utilizzo dell'istituto del trust come veicolo per la gestione dell'attività di emissione dei token. Gli Enti Blockchain, in aggiunta o in alternativa alla scelta di costituire una società di diritto sammarinese, potranno optare per l'istituzione di un apposito trust che avrà la funzione di gestire l'emissione di token e i rapporti con gli investitori ponendosi, tuttavia, come unico interlocutore nei confronti del soggetto emittente. Il trust consente una gestione patrimoniale puntuale, un elemento di garanzia rispetto alle esigenze di trasparenza che queste attività richiedono. Quello sammarinese è un modello di trust particolarmente apprezzato nel mondo, perché le leggi che lo regolano sono di semplice applicazione e avvicinano la Repubblica di San Marino alla cultura giuridica anglosassone, molto comprensibile anche dal punto di vista del linguaggio.

Anche la disciplina fiscale e contabile proposta da San Marino si pone in vantaggio rispetto ai Paesi che, a oggi, sono considerati come le migliori giurisdizioni in cui effettuare offerte di token e nelle quali si registrano il maggior numero di operatori blockchain.

Il nuovo Decreto, in particolare, ricorre a un meccanismo di assimilazione, sotto il profilo sia fiscale sia contabile, che considera i token di utilizzo come valute estere e quelli di investimento come azioni, strumenti finanziari partecipativi o titoli di debito dell'emittente a seconda dello strumento sottostante. Questo criterio consentirà di conoscere esattamente il regime di tassazione a tutti gli investitori, senza margini di interpretazione, e garantirà l'attrattività del sistema.

Il Decreto Delegato Blockchain prevede infine anche un'esenzione fiscale ai fini IGR per quanto riguarda i redditi realizzati attraverso operazioni effettuate con i token disciplinati nella disposizione. La scelta di applicare importati incentivi fiscali, anche in termini di defiscalizzazione totale, è stata adottata anche da altri Paesi, ma con specifico riguardo alle criptovalute e non per le altre tipologie di token. Il nuovo Decreto consentirà di attrarre investitori a San Marino, ma non di aprire il mercato indiscriminatamente, grazie

alla valutazione molto rigorosa, in termini di qualità, dei capitali che verranno "lasciati entrare", con opportune verifiche in forma rafforzata e presidi antiriciclaggio.

3.6 Malta

Con l'atto denominato *"Malta Digital Innovation Authority Act" ("MDIA Act")* del luglio 2018, il governo maltese ha posto un importante tassello per costruire la struttura normativa necessaria agli operatori del mondo blockchain.

Insieme alla MDIA Act, il governo maltese ha promulgato altri due atti che sono denominati:

– Innovative Technology Arrangement and Services Act ("ITAS Act");

– Virtual Financial Assets Act ("VFA Act").

Le 3 leggi che regoleranno la DLT (*distributed ledger technology*) sono state approvate dal Parlamento e convertite in legge[80]. Malta, è stata la prima giurisdizione al mondo a fornire certezza legale a questa realtà.

Dunque, con il *"Malta Digital Innovation Authority Act"* viene istituita la Malta Digital Innovation Authority con alla base 3 semplici principi guida riguardanti la blockchain:

- pieno rispetto dell'importanza di non ostacolare l'innovazione e gli sforzi e il potenziale del settore start-up;
- il riconoscimento e la regolamentazione sarà moderato dal ritmo di cambiamento e sviluppo che si sta verificando;
- garantire l'esistenza di standard per la tutela dei consumatori e degli investitori.

Mentre l'*"Innovative Technological Arrangement and Services Act"* definisce la tecnologia del registro decentralizzato (blockchain) in ogni sua parte compresi gli smart contract che vengono così definiti:

[80] Malta è l'unico paese al mondo ad avere tre leggi di rango primario sulla materia blockchain. Altri paesi come la Svizzera e Singapore hanno delle regolamentazioni ma sono scarne e settoriali, dedicate soltanto ad alcuni aspetti e quindi possono essere sovvertite da chiunque prenda una decisione diversa. Dunque, Malta oggi rappresenta il benchmark, la pietra di paragone, di tutti i legislatori del mondo.

- un protocollo elettronico; e, o

- un accordo concluso interamente o parzialmente con un modulo elettronico che è automatizzabile e attuabile mediante l'esecuzione di un codice informatico, sebbene alcune parti possano richiedere input e controlli umani e che possano essere applicabili anche con metodi legali ordinari o con una combinazione di entrambi.

Infine, con il *"Virtual Financial Asset Act"* vengono regolamentate le offerte iniziali di asset digitali i quali vengono così classificati:

- token virtuale

- bene finanziario virtuale

- moneta elettronica; o

- uno strumento finanziario

È molto interessante analizzare i notevoli poteri attribuiti all'Autorità: la stessa infatti può entrare ed ispezionare la residenza nonché ogni altro luogo dove vengono compiute delle attività che sono disciplinate dal MDIA Act stesso (Art. 40(1)(a)). Può inoltre richiedere documenti e sequestrarli ("remove and retain") o ordinare ai soggetti coinvolti di conservarli per il periodo che l'Autorità può ritenere necessario.

La struttura legale di Malta si è concentrata, dunque, sulla ricerca di un equilibrio tra l'innovazione e la regolazione, creando un sistema sufficiente a fornire garanzie alle parti interessate senza rovinare lo sviluppo del mercato con una regolamentazione eccessiva.

La legge maltese si focalizza sulla regolamentazione di una varietà di ICO che emettono token i quali possono essere classificati come Virtual Financial Asset (VFA), e ha creato una classe di licenze che regolerà la fornitura di servizi relativi ai VFA. Nessuna delle precedenti influirà sull'applicazione della legislazione esistente, come la MiFID che regola i servizi di investimento, o la direttiva di moneta elettronica che continuerà a governare i token che si qualificano come "e-money".

La struttura normativa maltese non dipende dalla speculazione. È completamente distaccata dall'imprevedibilità del mercato delle criptovalute ed in effetti ha come obbiettivo principale l'eliminazione delle congetture e la pratica di effettuare investimenti di crypto ad alto rischio con poca consapevolezza.

Guardando avanti, la struttura maltese è abbastanza ampia nella sua interpretazione per incapsulare molte innovazioni tecnologiche che possono essere la realtà di domani, come ad esempio gli smart contract e l'intelligenza artificiale. Questo garantisce che Malta sia attrezzata non solo a regolamentare la Blockchain così come esiste oggi, ma anche di tenere il passo con lo sviluppo costante della tecnologia, senza la necessità di costanti revisioni legali. Malta si configura quindi come valida soluzione per il mercato di oggi e per quello di domani.

3.7 Gibilterra

La *Gibraltar Financial Services Commission* (GFSC, la Consob di Gibilterra) ha annunciato che il suo regolamento su Blockchain, o Distributed Ledger Technology (DLT)[81], è in vigore dal 1° gennaio 2018. Da quest'anno, quindi, le aziende che utilizzano Blockchain per trasmettere o conservare valore, indipendentemente dal tipo di servizio, devono essere autorizzate da GFSC.

Nicky Gomez, responsabile rischio e innovazione di GFSC, ha commentato le nuove regole; "Siamo davvero entusiasti di ricevere finalmente le applicazioni dai provider DLT. Il team si aspetta di essere molto impegnato nei prossimi mesi e non vede l'ora di lavorare su alcune idee interessanti e innovative con i candidati. Lavorando a stretto contatto e in collaborazione con l'industria dei servizi finanziari e il governo di Gibilterra, il GFSC è diventato il primo regolatore a introdurre un quadro normativo su DLT ".

Si tratta del primo esempio di quadro legislativo appositamente costruito per le aziende che utilizzano la tecnologia blockchain o distributed ledger.

"Gibilterra si è posizionata come regime favorevole all'innovazione relativamente alla tecnologia Blockchain/DLT ed è un centro di eccellenza per il lancio di ICO".

[81] Il governo di Gibilterra ha introdotto delle norme che disciplinano la tecnologia blockchain e sta introducendo un testo di legge per regolamentare le ICO. Inoltre, considera l'opportunità di stabilire nuove norme riguardanti la vendita e la promozione di token.
Nell'ottobre 2017 è stato introdotto il *"Financial Services (Distributed Ledger Technology Providers) Regulations 2017"*. Tale regolamentazione è entrata in vigore a partire dal primo di gennaio 2018 e copre le imprese che operano all'interno del paese attraverso la blockchain. Esse vengono definite dalla presente legge quali l'esercizio di attività commerciali da o verso Gibilterra che operano attraverso la blockchain per archiviare o trasmettere valori appartenenti ad altri.

Gibilterra ha pubblicato un documento di consultazione sull'argomento nel maggio dell'anno scorso aggiungendo che nel valutare qualsiasi domanda di licenza i suoi obiettivi principali sono la protezione del consumatore e la reputazione di Gibilterra.

3.8 Il quadro giuridico della Svizzera

Il Consiglio federale svizzero ha pubblicato un *legal framework* dedicato al quadro giuridico per la *Distributed Ledger Technology (DLT)* nel settore finanziario. In questo report si afferma che il quadro giuridico svizzero è già adatto ad affrontare modelli di business basati su DLT e blockchain, ma che sono necessari diversi adeguamenti.

A tal proposito è interessante notare come, in alcuni ambiti specifici, non vi sia necessità di aggiustamenti ed in particolare sul tema delle definizioni terminologiche e dei principali processi coinvolti.

Il Consiglio federale "vuole creare le migliori condizioni possibili affinché la Svizzera possa affermarsi ed evolversi come sede principale, innovativa e sostenibile per le imprese del settore finanziario e Blockchain e, più in generale, per le imprese cosiddette innovative". Allo stesso tempo viene attribuita grande importanza alla garanzia dell'integrità e della reputazione della Svizzera come financial center e business location.

Il Paese è dichiaratamente favorevole al fenomeno delle ICO ed ha addirittura creato delle apposite zone territoriali, *cd. cryptovalley*, in cui vengono applicati dei regimi fiscali agevolativi allo scopo di attrarre aziende e startup in ambito blockchain. Già nel mese di febbraio 2018 *l'Autorità Federale di vigilanza sui mercati finanziari* (FINMA)[82] pubblicava delle linee guida in merito alle *Initial Coin Offering*, al fine di fornire un supporto interpretativo in merito agli adempimenti necessari per promuovere tali iniziative nello Stato svizzero. La FINMA con tale provvedimento introduceva una categorizzazione dei token distinguendoli sulla base dei diritti che essi conferiscono al loro titolare, secondo la tripartizione in *token di pagamento, utility token e security token.*

[82] La FINMA si adopera in seno a organismi internazionali per difendere gli interessi della Svizzera alla creazione di condizioni quadro che favoriscano gli sviluppi innovativi e alla garanzia di un adeguato livello di protezione dei clienti e del sistema. La FINMA ha inoltre concluso accordi di cooperazione nel settore della tecnofinanza con l'Australia e Israele.

Le offerte relative a tale ultima tipologia secondo le richiamate Linee Guida devono considerarsi soggette al regime di autorizzazione preventiva da parte dell'Autorità ed in ogni caso gli emittenti devono adempiere alle previsioni contenute nella normativa a contrasto del riciclaggio del denaro.

Successivamente nel mese di settembre 2018, in considerazione delle difficoltà riscontrate dalle banche svizzere per consentire l'apertura di conti correnti ai soggetti che avevano avviato operazioni di ICO, soprattutto per l'assenza in molte ipotesi del rispetto degli obblighi di identificazione degli investitori secondo la KYC, l'associazione delle banche svizzere ha pubblicato un'apposita guida pratica. Infine, nel mese di marzo 2019, in conseguenza dell'approvazione da parte del Parlamento svizzero di una nuova categoria di autorizzazione per le imprese *fintech* e dell'adeguamento degli spazi esenti dall'ambito autorizzatorio (cd. *sandbox*) l'Autorità di vigilanza ha avviato un'indagine conoscitiva per l'adeguamento delle circolari emesse che disciplinano tali aspetti.

3.9 Liechtenstein

Il Liechtenstein si allinea alla Svizzera con la legge *"Trusted Technologies*", un atto legislativo completo relativo alle DLT, ai token e al loro trattamento legale.

Il 7 maggio 2019 il governo del Liechtenstein ha riferito di aver approvato una mozione per implementare una nuova legge su token e fornitori di servizi VT (generalmente denominata "Blockchain Act").

In tempi recenti abbiamo visto varie giurisdizioni europee introdurre regolamenti o pubblicare linee guida normative su aspetti specifici delle tecnologie blockchain, tuttavia, il Liechtenstein ritiene che la sua Blockchain Act sia la prima a creare un quadro normativo olistico per l'economia dei token. Il motivo che il governo del Liechtenstein ha dato per adottare un approccio più olistico è quello di evitare di regolare specifiche applicazioni attuali in modo frammentario, in particolare criptovalute e offerte di monete iniziali, e invece mira a promuovere la certezza del diritto per le applicazioni che verranno create in futuro o stanno appena iniziando a emergere. Tuttavia, il governo del Liechtenstein si è espressamente riservato il diritto di regolamentare in modo specifico le applicazioni relative ai mercati finanziari in futuro.

Il Blockchain Act è stato redatto in senso lato e non utilizza il termine "blockchain", invece utilizza il termine "sistemi di transazione basati su tecnologie affidabili (sistemi VT)" come modo per descrivere i sistemi blockchain come Ethereum. Il governo del Liechtenstein spera che questo uso di una terminologia più astratta consentirà loro di essere a prova di futuro e mantenere la legge valida per le prossime generazioni di tecnologia e consentire l'interpretazione flessibile all'interno di un quadro normativo leggero.

La Blockchain Act consente a tutte le attività possibili, inclusi immobili, obbligazioni e titoli, di essere tokenizzate, digitalizzate e quotate in uno scambio di criptovaluta. La legislazione regola inoltre:

- la proprietà di risorse digitali (ovvero token);

- il trasferimento della proprietà delle risorse digitali;

- la conservazione sicura delle risorse digitali;

- requisiti legali per la conservazione di risorse digitali;

- diversi livelli di licenza per i fornitori di imprese nell'economia dei token; e

Offerte di token di sicurezza (STO), offerte di monete iniziali (ICO), vendite di token ed eventi di generazione di token (TGE).

La Blockchain Act è integrata dalle leggi sui servizi finanziari esistenti, comprese quelle relative ai requisiti KYC e AML.

L'obiettivo primario del governo del Liechtenstein per la Blockchain Act è fornire una chiara base giuridica per i fornitori di tecnologie blockchain al fine di garantire una maggiore certezza del diritto per tali fornitori e aumentare la fiducia dei loro clienti e utenti. Si spera che la Blockchain Act promuova l'obiettivo del Liechtenstein di diventare un hub di innovazione chiave per le nuove tecnologie creando buone condizioni quadro per le società blockchain e l'economia dei token.

La ricezione della Blockchain Act è stata mista. I critici hanno sostenuto che la velocità dei progressi tecnologici potrebbe far sì che gli sforzi per regolare l'economia dei token diventino rapidamente obsoleti nei prossimi anni, nonostante i tentativi del Liechtenstein di rendere il regolamento a prova di futuro facendo riferimento alle tecnologie fiduciarie. I critici hanno anche suggerito che, a causa della natura senza confini dell'ecosistema

blockchain / DLT, è necessario un maggiore sostegno a livello globale per ricevere l'adozione e l'accettazione in tutto il mondo, quindi la normativa nazionale potrebbe non essere da sola sufficiente a modificare comportamento del mercato nazionale.

Bibliografia

Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World, Paperback – June 12, 2018.

Satoshi Nakatomo, "*Bitcoin: A peer-to-Peer Electronic Cash System",* 2008. (https://bitcoin.org/bitcoin.pdf).

De Collibus F. M., Mauro R., "*Hacking Finance – la rivoluzione del bitcoin e della blockchain*", Milano, Agenzia X, 2016.

Dai W., *B-Money*, in http://www.weidai.com/bmoney.txt, 1998.

North C. D., "*Istituzioni, cambiamento istituzionale, evoluzione dell'economia"*, Il Mulino, 27 maggio 1994.

Topscott D. e A., "*Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World"*, Paperback, 12 giugno 2018.

Chohan, Usman W., Cryptocurrencies: A Brief Thematic Review (August 4, 2017). Disponibile su SSRN: https://ssrn.com/abstract=3024330 o http://dx.doi.org/10.2139/ssrn.3024330.

Michkin F. S., Eakins S. G., Forestieri G., "*Istituzioni e mercati finanziari",* Pearson Italia, 1 settembre 2015.

Tapscott D., "*How the blockchain is changing money and business"*, TEDSummit, giugno 2016.

Warburg B., "*How the blockchain will radically transform the economy"*, TEDSummit, giugno 2016.

Francesca A., "*Blockchain e smart contract: funzionamento e applicazioni"*, Altalex.com, 29 aprile 2019.

Bellini M., "*Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia"*, Blockchain4innovation.it, 26 settembre 2019.

Cataldo A., Campara F., "*Blockchain, criptovalute, smart contract, industria 4.0",* Pacini Editore, 2019.

Valsecchi V., *La classificazione delle Blockchain: pubbliche, autorizzate e private*, in Spindox.it, 20 giugno 2018 (https://www.spindox.it/it/blog/la-classificazione-delle-blockchain/#).

Mancini N., "*Bitcoin rischi e difficoltà normative"*, in Banca Impresa e Società, p.112, 2016.

Provenzani F**.,** *Cos'è il Proof Of Work (PoW) e Proof Of Stake (PoS)*, Money.it, 29 aprile 2019 (https://www.money.it/Cos-e-la-Proof-Of-Work-PoW-e-Proof-of-Stake).

Garavaglia R., "*Tutto su Blockchain. Capire la tecnologia e le nuove opportunità"*, Milano, 2018.

Banca Centrale Europea, "*Virtual Currency Schemes"*, febbraio 2015.

Pellizzari T., Morini M., "*il boom di Bitcoin non è per tutti"*, Il sole 24 ore, 27 novembre 2017.

Tupponi M., "*Manuale di diritto commerciale internazionale"*, G. Giappichelli Editore, Torino, 2019.