UNIVERSITÀ POLITECNICA DELLE MARCHE
FACOLTÀ DI ECONOMIA "GIORGIO FUÀ"

Corso di Laurea Magistrale o Specialistica in Economia e Management

BLOCKCHAIN E IMPATTI ECONOMICO-AZIENDALI

BLOCKCHAIN AND ECONOMIC-BUSINESS IMPACTS

Relatore: Chiar.mo
Prof. Marco Giuliani

Tesi di Laurea di:
Ludovica Raschioni

Anno Accademico 2019 – 2020

INDICE

INTRODUZIONE

Quello della fiducia è un problema che la nostra civiltà si trova a dover affrontare da circa diecimila anni. Nel 1400 il problema lo avevano risolto gli indigeni dell'Isola di Yap, in Micronesia, quando decisero di salire sulle loro zattere per vedere cosa ci fosse oltre l'Oceano. Si fermarono quindi sulla terraferma a loro più vicina, l'Isola di Palau, dove trovarono cose che non avevano mai visto nella loro piccolissima terra: tra le tante, rimasero stupiti di alcune pietre denominate "Rai", a tal punto da iniziare apposite spedizioni per portarle sulla loro Isola. Qualche anno dopo iniziarono ad avere il bisogno di una moneta (che non avevano mai avuto fino a quel momento), quindi di trovare un modo per standardizzare il valore. Decisero di utilizzare, in qualità di moneta, l'oggetto di cui allora disponevano maggiormente, il Rai appunto, non dandogli un valore in base a ciò con cui fosse stato costruito, ma in base alla sua storia: se, per esempio, il sasso era piccolo ed era stato facilmente raccolto e trasportato valeva poco, se il sasso era molto grande ed erano morte delle persone nella spedizione per riuscire a portarlo sull'Isola valeva tantissimo. Ad ogni modo, non importava possedere fisicamente il Rai: gli abitanti dell'Isola ebbero l'intuizione di introdurre ed applicare un codice di regolamento secondo il quale ogni singolo individuo dovesse possedere una copia del registro unico decentralizzato che riportava tutte

le informazioni circa la storia e la proprietà dei sassi. Dunque non importava che il proprietario possedesse fisicamente il Rai o, ancora, che gli fosse stato rubato: per poterlo spendere bastava che l'informazione che ne attestava la proprietà fosse contenuta all'interno del registro distribuito a tutti gli abitanti dell'Isola.

Il grande cambiamento di paradigma consistette nel fatto che il valore non era più intrinseco nell'oggetto scambiato -come non lo è di certo nemmeno oggi-, ma era nell'informazione condivisa tra tutte le persone dell'Isola. E oggi, dopo più di 600 anni, stiamo rivivendo questa storia, perché possediamo una tecnologia, la Blockchain, che non è altro che un database distribuito, decentralizzato e condiviso tra i partecipanti di una rete.

La Blockchain, annoverata tra le Distributed Ledger Technologies, viene oggi divulgata da molti esperti come la più importante innovazione tecnologica dell'odierna economia, capace di stravolgere la tradizionale logica centralizzata in favore di un nuovo "ecosistema di fiducia", decentralizzato e distribuito.

La presente Tesi di Laurea ha l'obiettivo di introdurre l'universo Blockchain partendo dal bitcoin, la più famosa delle cryptocurrency. Blockchain è stata infatti inizialmente sviluppata per la stessa in qualità di registro distribuito gestito da una rete *peer-to-peer* di partecipanti. Più nello specifico, applicata al contesto dei bitcoin, la Blockchain è un registro decentralizzato che contiene i dettagli di ogni transazione BTC che sia mai stata completata. Utilizzando dispositivi che eseguono algoritmi sofisticati, alcuni utenti della rete, denominati *miners*, creano

dei blocchi all'interno dei quali vengono inserite le transazioni giudicate valide, assicurando pertanto un elevato grado di precisione e sicurezza[1]. Ogni operazione è così permanentemente registrata sulla Blockchain, creando un registro sempre crescente di attività: il continuo monitoraggio da parte di tutti i computer della rete ne garantisce l'affidabilità e la robustezza. Con decine di migliaia di nodi che verificano ogni transazione, una collusione per sovvertire il sistema diventa pertanto difficile e costosa.

A seguito di una disamina iniziale dei principali riferimenti teorici funzionali alla comprensione della Blockchain, il secondo capitolo della trattazione si occuperà di descrivere nel dettaglio le caratteristiche e le modalità di funzionamento della Tecnologia. L'elaborato vuole infatti fornire uno strumento informativo che permetta di maturare una comprensione dell'argomento che ad oggi in letteratura economica e nella cronaca giornalistica risulta tanto dibattuto quanto presentato in maniera frammentaria e talvolta poco esaustiva.

Ma il vero interesse per la Blockchain è esploso quando è apparso chiaro che essa poteva essere utilizzata per documentare il trasferimento di qualsiasi asset digitale, registrare proprietà sia fisiche che intellettuali, creare una nuova tipologia di contratti più efficiente e sicura -gli *smart contracts*-, semplificando notevolmente il processo di creazione ed esecuzione degli stessi. Il terzo capitolo della presente

[1] Nel caso di Bitcoin, gli nodi della rete sono pagati per il loro lavoro di verifica delle transazioni da inserire nella Blockchain.

trattazione sottolinea, pertanto, l'importanza assunta dalla Blockchain nel business: l'introduzione della stessa è in grado di rivoluzionare il modus operandi di un'azienda, impattando sul modello di business, sulla strategia, nonché su governance, mission e vision di ciascuna.

L'uso della Blockchain, dunque, non è limitato al settore finanziario: l'obiettivo del quarto ed ultimo capitolo, a seguito di una breve disamina della normativa vigente, è proprio quello di sottolineare gli attuali impatti della Tecnologia nei vari settori economici, nonché quello di riflettere sulle potenziali applicazioni future della stessa. Nonostante le polemiche, il modello Blockchain, attraverso il consenso digitale massicciamente distribuito, è una scoperta che potrebbe ridisegnare il commercio nell'intera economia digitale.

CAPITOLO 1

DA BITCOIN A BLOCKCHAIN

1.1 Le criptovalute

Quando ci riferiamo ai nuovi strumenti di pagamento definiti "criptovalute", molto spesso cadiamo in errore relativamente alla terminologia utilizzata per delinearle. Nel linguaggio comune si fa solitamente riferimento ai termini "valuta virtuale" e "valuta digitale" utilizzandoli come sinonimi: in realtà, però, almeno originariamente, tra i due vi è differenza. Le valute virtuali sono un tipo di valuta digitale, ma non può dirsi il contrario[2]. Di fatti, poiché non esiste fisicamente, il denaro virtuale esiste solo nel suo formato digitale: ad esempio, molti videogiochi utilizzano una valuta, appunto virtuale, con cui è possibile acquistare oggetti all'interno del gioco. La valuta digitale, di contro, è la rappresentazione digitale di tutti i tipi di valute, utilizzate per effettuare pagamenti di beni e servizi. Un esempio di questo tipo di valuta è quella che viene memorizzata nei conti bancari, con i quali è possibile effettuare trasferimenti elettronici, pagamenti con carte di

[2] Fonte: Capaccioli S., "*Criptovalute e bitcoin: un'analisi giuridica*", Giuffrè Editore, 2015.

debito e di credito. E le varie criptovalute[3], pur ricadendo nell'ampio insieme delle valute digitali, differiscono dalle stesse: propriamente sono valute memorizzate e scambiate in maniera elettronica, ma che rispetto alle valute digitali non sono denominate in moneta avente corso legale (*fiat money*) e possiedono pertanto una propria unità di conto[4].

Per comprendere al meglio le differenze tra criptovalute e valute digitali, è necessario evidenziarne le ulteriori caratteristiche. Mentre le valute digitali sono centralizzate, cioè esiste un'autorità centrale che ne disciplina lo stato delle transazioni, le criptomonete sono *decentralizzate*, il che implica che la regolamentazione delle transazioni sia attuata dalla comunità medesima. In secondo luogo, al contrario delle monete digitali, le criptovalute sono *trasparenti*: chiunque può consultare l'elenco delle transazioni effettuate, poiché il flusso del denaro viene inserito in una catena pubblica (blockchain). Ulteriore grande distinzione riguarda l'emissione della moneta: quella della criptovaluta non è regolata da un'entità che ne controlla la quantità e la modalità.

Com'è quindi intuibile, l'innovazione introdotta dalle criptovalute si evidenzia nel fatto che queste ultime sono costituite da un processo che incorpora i principi

[3] Una criptovaluta è definita come una *rappresentazione digitale di valore*, la cui proprietà è mantenuta da una blockchain che la utilizza come strumento di pagamento per compensare gli appartenenti al network e mantenere l'integrità del sistema stesso. Fonte: D. Drescher, *"Blockchain Basics: A Non-Technical Introduction in 25 Steps",* Apress, 2017.

[4] Fonte: Dong He *et al*., "*IMF staff discussion note: Virtual Currency and Beyond: initial considerations*", Gennaio 2016.

della crittografia con una valuta virtuale decentralizzata e quasi sempre limitata nella quantità totale di emissione[5].

È possibile a questo punto riassumere le differenti classificazioni di valuta proposte utilizzando una raffigurazione secondo la quale ogni gruppo superiore contiene al suo interno quelli a sé inferiori (*figura 1*).

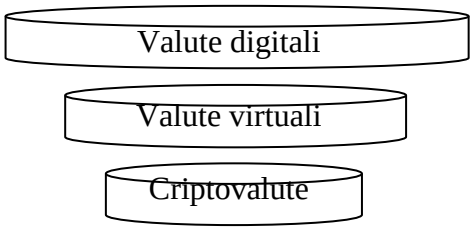

Figura 1. Classificazione grafica delle valute. Fonte: elaborazione dell'autore.

Risulta pertanto di facile comprensione il fatto che tutte le criptovalute sono moneta virtuale e moneta digitale, ma non viceversa.

Il concetto di criptovaluta è apparso per la prima volta con la pubblicazione di un articolo[6] di David Chaum che introdusse le cosiddette "*firme cieche*", dall'inglese "*blind signatures*": queste sono da intendere come firme digitali che vengono apposte su un messaggio prima che quest'ultimo venga aperto e letto. Il nome dell'autore è infatti associato all'invenzione della *Blind Signature Technology*,

[5] Il fatto che la quantità di emissione della moneta sia predefinita non è fattore caratterizzante della totalità delle criptovalute esistenti ma è elemento determinante nella grande maggioranza delle stesse.

[6] Fonte: David Chaum, "*Blind Signature for Untraceable Payments*", 1982.

progettata per garantire la completa privacy degli utenti nelle transazioni online: il suo obiettivo fu quello di impedire ad una banca o ad un'autorità governativa pubblica di poter tracciare i pagamenti e gli acquisti effettuati su Internet.

Nello specifico, è attribuita a David Chaum la fondazione della *DigiCash Inc.*, una società informatica attiva dal 1989 nell'ambito della moneta elettronica e della gestione dei pagamenti online. La corporazione fondata da Chaum vedeva la sua innovazione nei sistemi di transazioni monetarie online: gli utenti potevano concludere transazioni usando un software proprietario (*Ecash*) che permetteva di "prelevare" moneta da una banca attraverso l'uso di chiavi crittografiche. Per la prima volta le transazioni erano anonime ed associate ad un codice crittografico, all'interno di un sistema centralizzato (*figura 2*). Di fatto, *DigiCash* è stata una delle prime compagnie sostenitrici della crittografia a chiave pubblica e privata, lo stesso principio di base utilizzato oggi dalle criptovalute.

Sebbene David Chaum avesse compiuto il primo passo, ancora non bastava: le transazioni erano anonime e digitali, ma richiedevano comunque il passaggio attraverso *DigiCash* stessa ed una banca, il che non rientrava nel concetto di decentralizzazione delle transazioni voluto dal creatore di Bitcoin vent'anni più tardi.

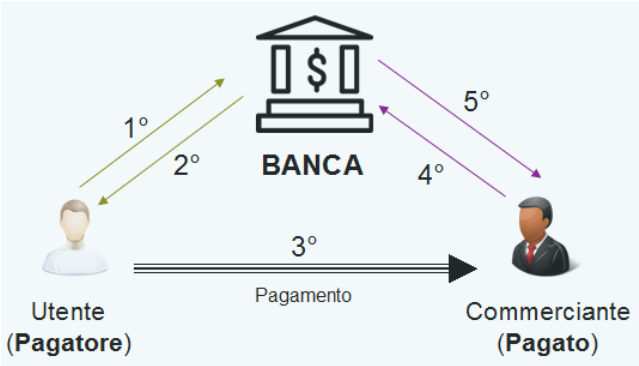

Figura 2. Software Ecash. Fonte: www.portagolioelettronicomigliore.com.

La *DigiCash Inc.* dichiarò bancarotta qualche anno più tardi, nel 1998: un ostacolo al suo potenziale successo è stato il fatto che una serie di accordi con banche e società di carte di credito non siano andati a buon fine. Se la società fosse riuscita a garantire una partnership con uno o più importanti istituti finanziari avrebbe avuto maggiori probabilità di sopravvivere nel mondo finanziario in rapida digitalizzazione.

Nello stesso anno del fallimento della *DigiCash*, Wei Dai, un esponente del gruppo Cyberpunk[7], proponeva un trattato[8] per la presentazione di un nuovo sistema di pagamento anonimo e distribuito. Nella fattispecie, si trattava di un sistema di interscambio di valore e stipulazione di contratti che si basava sull'uso

[7] Per Cyberpunk si fa riferimento ad un movimento artistico e letterario sviluppatosi negli anni '80 per azione di un gruppo di attivisti che vedevano nelle tecnologie informatiche e nella cibernetica strumenti utili per un cambiamento radicale all'interno della società.
[8] Fonte: Wei Dai, "*B-money, an anonymous, distributed, electronic cash system*", 1998.

di una moneta digitale (la cosiddetta "*B-Money*") anonima, distribuita e decentralizzata.

Le idee di quest'ultimo fungeranno da base teorica per il successivo sviluppo delle criptovalute, e, nello specifico, della più famosa tra queste: il Bitcoin.

1.1.1 Nascita ed evoluzione del Bitcoin: cenni storici

Nel 2008 si concretizzò il contributo determinante per portare definitivamente alla ribalta il tema delle criptovalute, in seguito alla pubblicazione di un paper scientifico intitolato "*Bitcoin: A Peer-to-Peer Electronic Cash System*" per opera di Satoshi Nakamoto, pseudonimo dell'inventore del bitcoin[9]. Le teorie sulla vera identità di Satoshi Nakamoto sono numerose: nessuno sa se è un "lui", una "lei" oppure se si tratta di un gruppo di persone. La cosa certa è che l'obiettivo della sua mente geniale fu quello di creare un sistema di pagamento online, sicuro e indipendente dalle autorità centrali[10].

Il bitcoin, lanciato nel 2009 come metodo di pagamento virtuale, è definito infatti come "*la prima valuta digitale decentralizzata*"[11]. Come è ormai stato più volte

[9] Convenzionalmente, utilizzeremo il termine "Bitcoin" maiuscolo per riferirci alla tecnologia e alla rete, mentre il minuscolo "bitcoin" per far menzione della valuta in sé.
[10] Il sistema Bitcoin non fa uso di un ente centrale: esso utilizza un database distribuito tra i nodi della rete che tengono traccia delle transazioni, e sfrutta la crittografia per gestire gli aspetti funzionali come la generazione di nuova moneta e l'attribuzione di proprietà dei bitcoin. Fonte: www.bitcoin.org.
[11] Definizione offerta dal sito ufficiale www.bitoin.org.

sottolineato, si tratta della più famosa delle "cripto-valute": fonda cioè la sua costruzione su degli algoritmi crittografici tali da garantirne la sicurezza[12].

I bitcoin sono la moneta digitale che viene scambiata sull'omonima piattaforma, definibile come un registro digitale di transazioni che rende ogni spostamento di valuta pubblicamente visibile, garantendo allo stesso tempo l'anonimato delle transazioni grazie alla crittografia della valuta.

I pagamenti in bitcoin non richiedono intermediari né spostamenti fisici di valuta, e possono essere effettuati in qualsiasi momento verso persone o istituzioni in ogni parte del mondo: Bitcoin, di fatti, rappresenta un sistema di pagamento molto più economico e veloce di quello tradizionale, soprattutto per i trasferimenti internazionali, motivo per cui ha avuto grande consenso e diffusione, attraendo tutti coloro che desiderano fare acquisti sulla rete globale in modo più rapido rispetto a quanto permettano i sistemi tradizionali.

Un articolo della nota rivista americana "*Financial Times*", nel novembre 2017, racconta la storia di Erik Finman, ragazzo che riuscì in pochi anni a diventare milionario investendo appena 1000 dollari in Bitcoin. E proprio a fronte di tale accadimento ed esperienza, molti individui furono spinti, allo stesso modo, ad investire in bitcoin, senza sapere realmente su cosa: fu l'inizio della bolla speculativa, verificatasi nel 2017, che portò il bitcoin ad un valore unitario superiore a 20 mila dollari. In quanto alle ragioni della bolla, secondo

[12] Fonte: "*Bitcoin, cos'è e come funziona*", Borsa Italiana, 2019.

Bloomberg[13], esse vanno ricercate in una combinazione di comportamento del branco, speculazione cinica e ingresso nel mercato di un gran numero di nuovi investitori poco informati. Molti utenti, di fatto, vedendo i loro investimenti moltiplicarsi enormemente in breve tempo, decisero di ritirarsi dal mercato ed incassare. Ciò comportò il successivo crollo del 26 dicembre 2018: i bitcoin sono passati da 12.200 euro di gennaio ai 3.290 euro nel dicembre dello stesso anno[14].

Ma per uno strano meccanismo cripto-finanziario, mentre il bitcoin perdeva colpi, la rete su cui esso poggia e che ne permette la diffusione (la Blockchain) si è guadagnata un posto in primo piano nell'ormai attuale futuro come pilastro della quarta rivoluzione industriale. Di fatti, per quanto negativo per la madre di tutte le criptovalute, il 2018 è stato un anno fondamentale per la cripto-finanza e per la Blockchain, database decentralizzato usato per registrare le transazioni dei bitcoin, che, nonostante la debacle valutaria, ne è uscita trionfante.

I parametri tecnici del BTC hanno poi infranto nuovi record nel 2019: infatti, i dati evidenziano che dal punto di vista tecnico la criptovaluta ha raggiunto livelli inediti. Una disamina di tre parametri (numero di transazioni, volume delle transazioni e hash rate[15] di Bitcoin) ha confermato che il trend di bitcoin durante l'anno passato non è stato affatto ribassista. In primo luogo si rileva che la rete

[13] *Bloomberg* è una multinazionale operativa nel settore dei mass media che, crescendo nel corso degli anni, ha creato un servizio mondiale di news che comprende TV, agenzia di stampa, radio, internet e pubblicazioni editoriali.

[14] Fonte: Pierangelo Soldavini, "*Bitcoin in caduta libera perde il 30% in una settimana: le tre ragioni del crollo*", SOLE24ORE, 2018.

[15] Per hash rate si intende l'unità di misura della potenza di elaborazione della rete Bitcoin.

Bitcoin ha elaborato più transazioni nel 2019 che in qualunque altro anno: nel maggio dello scorso anno, definito come mese di maggiore attività in assoluto per Bitcoin, si sono registrate infatti ben 12 milioni di transazioni. In secondo luogo, *Blockchain.com* osserva che nell'anno precedente sulla rete Bitcoin è stato spostato più valore che mai prima: in particolare, è stato raggiunto un punto apicale pari a 4 miliardi di dollari in un solo giorno. E in ultimo si segnala il costante miglioramento dell'hash rate di Bitcoin nel corso dell'anno in esame.

Anche se alcuni, perlomeno inizialmente, erano scettici riguardo al successo di Bitcoin come strumento che potesse rivelarsi al pari della moneta, con il passare del tempo divenne evidente che, a prescindere dal possibile successo o meno in futuro di tale sistema (successo che poi, a livello di rendimenti realizzati e di notorietà mediatica, vi è sicuramente stato), la vera rivoluzione era la tecnologia che stava alla base della stessa valuta virtuale introdotta da Nakamoto: la cosiddetta Blockchain.

Prima di addentrarci nell'analisi della tecnologia Blockchain e dei meccanismi che ne regolano il funzionamento, nel seguente paragrafo proporremo dei presupposti teorici di base che ne aiuteranno la comprensione.

1.2 Struttura di un sistema

Quando ci riferiamo alla struttura di un sistema intendiamo la disposizione dell'insieme degli elementi singoli che lo compongono, che connessi tra loro formano un elemento unico e più complesso.

I tre tipi più comuni di struttura per un sistema sono:

1. Centralizzato
2. Decentralizzato
3. Distribuito

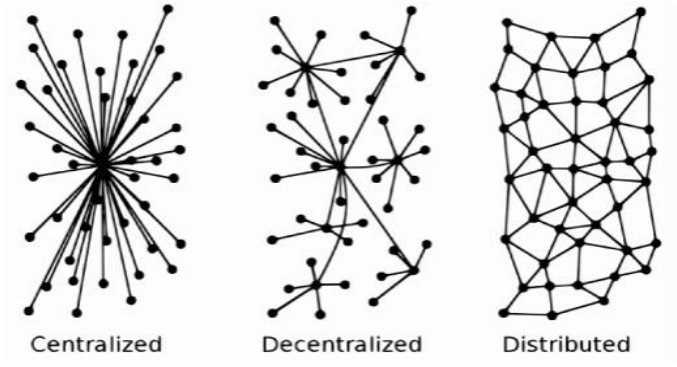

Figura 3. Strutture di un sistema. Fonte: "Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia", Mauro Bellini, 2020.

Un sistema *centralizzato* può essere meglio pensato come una struttura a "mozzo e raggi", dove un componente dominante si trova al centro e coordina gli altri componenti del sistema. La struttura proposta denota uno dei limiti principali di questo tipo di reti: l'eccessiva dipendenza di tutti i raggi (o partecipanti) nei

confronti del centro, che si riflette in una debolezza nel momento in cui il coordinamento tra i nodi[16] e l'hub[17] dovesse, per qualsiasi ragione, fallire.

Pertanto, un sistema *decentralizzato* cerca di correggere i difetti insiti in quelli centralizzati, creando appunto più hub e raggi. Come risulta chiaro dalla *figura 3*, in un sistema decentralizzato sono presenti molti nodi, ciascuno incaricato di garantire il flusso regolare del "traffico" (di informazioni, di messaggi, di regole, di transazioni finanziarie, ecc.). Tuttavia, in un sistema così strutturato i vari nodi, sebbene siano dotati di una certa autonomia, devono comunque fare riferimento ad un ente centrale.

Sotto questo profilo, un'evoluzione del sistema decentralizzato è rappresentata da quello *distribuito*, in cui ogni partecipante agisce come un hub: ogni individuo, computer o entità governativa che sia possiede uguale responsabilità e autonomia, assicurando il buon funzionamento del network stesso. Se un nodo del sistema fallisce, gli altri nodi semplicemente prendono il suo posto e si assicurano che il meccanismo di trasmissione, ovvero il flusso del "traffico", proceda regolarmente. Caratteristica denotabile dalla figura proposta è il fatto che non si rende

[16] In informatica un nodo è un qualsiasi dispositivo hardware del sistema in grado di comunicare con gli altri dispositivi che fanno parte della rete; può quindi essere un computer, una stampante, un fax, un modem, ecc.

[17] In informatica un hub (letteralmente in inglese fulcro, mozzo, elemento centrale) rappresenta un dispositivo di rete che funge da nodo di smistamento dati di una rete di comunicazione dati organizzata con una topologia logica a bus e una topologia fisica a stella.

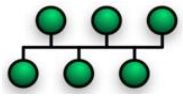

Figura 14.1: topologia a bus

Figura 14.2: topologia a stella

necessario, per il funzionamento di tale sistema, che i nodi della rete siano collegati tra loro in maniera diretta, ma è sufficiente che lo siano indirettamente.

Sistemi centralizzati e distribuiti, pur essendo strutturati in maniera opposta, possono essere combinati tra loro (*figura 4*): esistono infatti sistemi distribuiti in cui tutti i nodi della rete, oltre ad interagire reciprocamente, si rifanno ad un nodo centrale, e sistemi centralizzati in cui il centro è costituito da un insieme di nodi distribuiti, collegato a sua volta a nodi esterni ad esso.

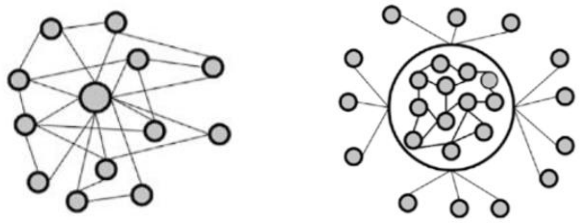

Figura 4. Strutture di sistemi ibridi. Fonte: D. Drescher, "Blockchain Basics: A Non-Technical Introduction in 25 Steps", Apress, 2017.

1.2.1 P2P: un sistema di comunicazione client-client

Soffermandoci sul sistema distribuito quale struttura maggiormente rappresentativa della tecnologia Blockchain, risulta opportuno e propedeutico esplicare una delle configurazioni tipo di tale sistema: quella "*peer-to-peer*". Nella sua forma più semplice, un network P2P (o "rete paritaria") si costituisce quando due o più computer possono scambiarsi informazioni senza dover passare

attraverso un calcolatore centrale che coordini il tutto. Pertanto, una rete *peer-to-peer* si basa su una de-gerarchizzazione dei nodi che la compongono: indica cioè un modello di architettura logica di rete informatica in cui i nodi non sono gerarchizzati unicamente sotto forma di client o server fissi, ma anche sotto forma di nodi equivalenti o "paritari" (*peer*), potendo fungere al contempo da client e server verso gli altri nodi della rete. Ogni computer che si connette ad una rete P2P, quindi, ha la possibilità di condividere i file archiviati sulle proprie memorie di massa e, al contempo, di accedere ai contenuti messi a disposizione dagli altri PC (*figura 6*). In altre parole, quando un nodo agisce da client scarica file da altri nodi nel network, quando invece opera in veste di server risulta essere la fonte da cui gli altri nodi possono scaricare file: questo è ciò che differenzia i network P2P dai più tradizionali sistemi client-server, in cui i dispositivi client scaricano file da un server centralizzato (*figura 7*).

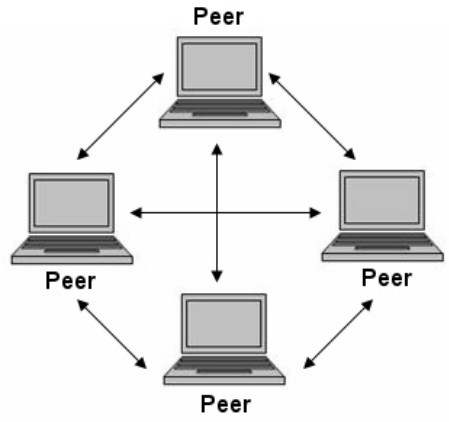

Figura 6. Architettura peer-to-peer. Fonte: www.nicom672.wordpress.com.

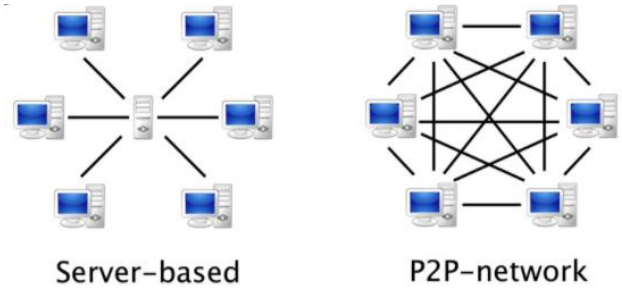

Figura 7. Differenza strutturale tra un sistema server-based e un P2P. Fonte: www.guardacome.com.

Per il funzionamento dei P2P-network, non essendoci un server centrale in grado di far connettere tra loro i diversi nodi, è fondamentale l'utilizzo di una cosiddetta rete sovrapposta (*overlay network*)[18]: si tratta di una rete virtuale costruita su quella fisica principale, che permette di mappare i diversi nodi in modo da rendere visibile la struttura della rete a tutti i partecipanti.

L'architettura P2P, diventata particolarmente popolare negli anni '90 con la creazione dei primi programmi per la condivisione di file, costituisce oggi la base di gran parte delle criptovalute, occupando un'importante fetta del settore della Blockchain. Nelle fasi iniziali di Bitcoin, Satoshi Nakamoto l'ha definito come un "Sistema di Moneta Elettronica Peer-to-Peer". Pertanto, i bitcoin, in qualità di moneta digitale, possono esser trasferiti da un utente all'altro proprio attraverso un network P2P, che gestisce un registro distribuito chiamato blockchain. In questo

[18] Generalmente, i nodi possono essere connessi fra loro tramite collegamenti logici o virtuali, ciascuno dei quali corrisponde ad un percorso nella rete sottostante. Sistemi distribuiti come appunto i *peer-to-peer* sono delle overlay network, poiché i loro nodi si sovrappongono a quelli della rete Internet.

contesto, l’architettura P2P, intrinseca alla tecnologia Blockchain, è ciò che permette al bitcoin (così come ad altre criptovalute) di essere trasferito in tutto il mondo, senza bisogno né di intermediari né di server centrali. In sintesi, non ci sono banche che elaborano o registrano transazioni nel network di Bitcoin, ma è la Blockchain ad agire come un registro digitale che archivia pubblicamente tutte le attività.

Per approfondimenti tecnici relativi alla tecnologia Blockchain si rimanda al capitolo successivo in cui, a fronte delle basi teoriche offerte nel presente, analizzeremo nel dettaglio la struttura, i meccanismi di funzionamento e i principali vantaggi della tecnologia in esame.

CAPITOLO 2

LA TECNOLOGIA BLOCKCHAIN

2.1 Introduzione alla Blockchain: caratteristiche e funzionamento

Generalmente quando si parla di Blockchain si parte dal Bitcoin: questo perché Bitcoin è stata la prima vera implementazione della tecnologia in esame, detenendo oggi il merito di averla resa famosa ed aver creato interesse intorno ad essa. Nello specifico, Blockchain è l'infrastruttura che sta alla base di Bitcoin e delle altre cryptocurrency, ovvero il meccanismo che le fa funzionare e che le rende così sicure[19].

Letteralmente la parola "**Blockchain**" significa "blocchi concatenati" e, anche se non esiste un'unica definizione, è possibile immaginarla come una concatenazione di **blocchi** costituiti dall'insieme delle **transazioni** verificabili e verificate dai nodi di una rete (formata fisicamente dai server di ciascun partecipante).

[19] "*Bitcoin è il primo vero prodotto concreto e operativo che per il suo funzionamento fa affidamento su questa tecnologia*". Fonte: Michele Faioli, Emanuele Petrilli, Donato Faioli, "*Blockchain, contratti e lavoro. La ri-rivoluzione digitale nel mondo produttivo e nelle PA*", 2019.

Una **transazione** è lo scambio di valore che avviene tra due partecipanti di un network, che rappresentano rispettivamente il *sender* e il *receiver*.

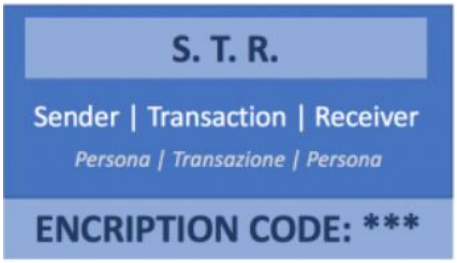

Figura 8. I componenti della transazione. Fonte: www.blockchain4innovation.it.

Un **blocco**, a sua volta, è formato da un insieme di transazioni: ne rappresenta quindi il raggruppamento fisico.

Figura 9. I blocchi come insieme di più transazioni. Fonte: www.blockchain4innovation.it.

Dall'unione di più blocchi, infine, si costruisce la **Blockchain**.

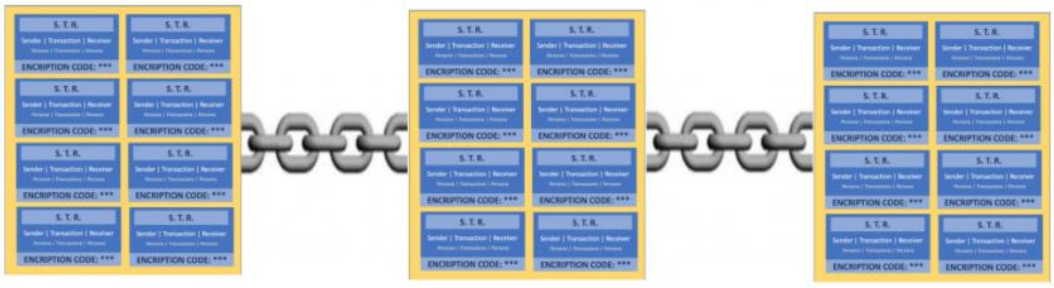

Figura 10. Rappresentazione grafica di una Blockchain. Fonte: www.blockchain4innovation.it.

La Blockchain si presta ad essere interpretata: più che una tecnologia è un paradigma, un modo di intendere il grande tema della decentralizzazione e della partecipazione[20]. Per questo ne esistono diverse declinazioni e interpretazioni. Una rassegna di definizioni può essere utile per capire come viene vissuta e interpretata in funzione della prospettiva di utilizzo.

Secondo una prima definizione la Blockchain è un **database di transazioni**[21]: "*è una tecnologia che permette la creazione di un grande database distribuito per la gestione di transazioni condivisibili tra più nodi di una rete*"[22]. Questa interpretazione fa riferimento, quindi, ad un database strutturato in blocchi tra loro collegati, ciascuno dei quali contiene più transazioni, che sono validate dai nodi

[20] Fonte: Michele Faioli, Emanuele Petrilli, Donato Faioli, "*Blockchain, contratti e lavoro. La ri-rivoluzione digitale nel mondo produttivo e nelle PA*", 2019.
[21] Fonte: D. LEE Kuo Chuen, R. H. DENG, "*Handbook of blockchain, digital finance and inclusion – volume 2*", Elsevier, 2018.
[22] Fonte: "*Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia*", Mauro Bellini, 2020.

della rete stessa nell'analisi che viene effettuata relativamente a ciascun blocco[23]. I blocchi rappresentano pertanto un archivio di tutte le transazioni avvenute, che possono essere validate, e quindi accettate, solo con l'approvazione dei nodi della rete stessa.

Altri studiosi pongono l'enfasi sul fatto che Blockchain è un **registro pubblico identicamente distribuito**[24], ossia uguale per tutti: la stessa "informazione" è infatti presente sui database di tutti i nodi della rete e diventa pertanto immodificabile se non attraverso una operazione che richiede l'approvazione della maggioranza dei nodi del network, operazione che in ogni caso non modificherà la storia di quella stessa informazione.

Per altri, ancora, la Blockchain esprime al meglio l'evoluzione del concetto di "*ledger*" ossia di "**libro mastro**"[25]. 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 (rappresentata dal tradizionale *centralized ledger*), secondo la quale tutto faceva riferimento ed era gestito da una singola unità o autorità, di cui 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 entità centrale, ma si

[23] Fonte: Osservatorio Blockchain & Distributed Ledger, "*Blockchain & Distributed Ledger: unlocking the potential of Internet of Value*", 2020.
[24] Fonte: "*Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia*", Mauro Bellini, 2020.
[25] Fonte: "*Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia*", Mauro Bellini, 2020.

sposta nelle "periferie", che assumono sempre più rilevanza nella transazione. Nello specifico, "*il decentralized ledger ripropone la logica centralizzata a livello locale con satelliti organizzati nella forma di uno-a-tanti che si relazionano a loro volta in una forma che ripete il modello uno-a-tanti: non esiste più un unico soggetto centrale bensì tanti soggetti centrali*"[26]. Ma la vera innovazione è rappresentata dal passaggio dal concetto di *decentralized ledger* a quello di *distributed ledger*: questo è l'aspetto più saliente della tecnologia Blockchain, di cui offriremo di seguito un approfondimento (*paragrafo 2.1.1*).

Se dare una o più definizioni di Blockchain può essere relativamente semplice, spiegare cosa è e a cosa serve può essere meno intuitivo di quello che si pensi: tenteremo quindi di offrire una comprensione del fenomeno piuttosto immediata analizzando, in modo logico e sequenziale, gli aspetti caratterizzanti della tecnologia in esame. Nello specifico, approfondiremo i concetti chiave che seguono:

- La **DLT** (*Distributed Ledger Technology*), ovvero quella famiglia di tecnologie basate su un "registro distribuito" (*distributed ledger*) tra i partecipanti di una rete;
- La **crittografia**, che gestisce la sicurezza dei dati e delle transazioni all'interno del network;

[26] Fonte: Osservatorio Blockchain & Distributed Ledger, "*Blockchain & Distributed Ledger: unlocking the potential of Internet of Value*", 2020.

- Il meccanismo di **consenso**, che, nel caso di BC, permette di gestirne il controllo in modo trasparente e senza intermediari;
- La **gestione dei dati**, che funziona in maniera "*append-only*"[27], garantendo cioè persistenza e integrità poiché la BC non permette di eliminare o modificare i dati esistenti in piattaforma;
- **The double spending problem** (problema della "doppia spesa"), cui la BC pone rimedio, non ammettendo la possibilità di utilizzare, e quindi spendere, lo stesso titolo valutario due o più volte.

2.1.1 Blockchain come Distributed Ledger Technology

Le tecnologie *Distributed Ledger* sono sistemi basati su un **registro distribuito**, ossia sistemi in cui tutti i nodi di una rete possiedono la medesima copia di un database, che può essere letto e modificato in modo indipendente dai singoli nodi[28]. E le tecnologie Blockchain sono incluse nella più ampia famiglia delle *Distributed Ledger Technologies* (DLT).

Nello specifico, il *ledger*, in qualità di "libro mastro", rappresenta di fatti il modo di interpretare e gestire le relazioni e le transazioni tra persone e tra organizzazioni, sin dai tempi in cui, grazie alla scrittura, la nostra civiltà ha

[27] Allude, nello specifico, alla sola possibilità di aggiungere, all'interno della BC, dati ed informazioni, escludendo quindi l'ipotesi di poter eliminare o manipolare dati esistenti.
[28] Fonte: Massimiliano Nicotra, Fulvio Sarzana di S. Ippolito, "*Diritto della blockchain, intelligenza artificiale e IoT*", 2018.

iniziato a lasciare una memoria delle proprie azioni a carattere commerciale e degli scambi tra due o più parti. Tale registro ha un valore nel momento e nella misura in cui può essere consultato per controllare, verificare e gestire le transazioni e gli scambi effettuati[29], fungendo da vera e propria memoria storica.

Il concetto di un libro mastro distribuito in copie uguali ad una moltitudine di persone consente di introdurre una nuova logica di 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 quella basata sulla fiducia tra tutti i partecipanti, ognuno dei quali ha le stesse informazioni degli altri[30].

Al giorno d'oggi, le transazioni effettuate, ovvero il passaggio di proprietà di denaro o attività finanziarie tra utenti, avvengono attraverso sistemi centralizzati, gestiti solitamente dalle banche centrali. Le banche tengono traccia delle transazioni in database locali, i quali vengono aggiornati una volta che un'operazione è stata eseguita nel sistema centralizzato.

"*Un distributed ledger è invece un database di operazioni distribuito su una rete di numerosi computer, anziché custodito presso un nodo centrale*"[31]: tutti i membri della rete possono leggerne le informazioni e, a seconda dei permessi di cui dispongono, possono anche aggiungerne.

---

[29] Fonte: "*Blockchain ed energy sharing: una rivoluzione nel campo dell'energia*", Avv. Marco Del Fungo, 2018.

[30] Fonte: "*Le nuove sfide della proprietà intellettuale: Blockchain e Smart Contract*", Studio Legale Saglietti-Bianco, 2019.

[31] Fonte: sito ufficiale Banca Centrale Europea.

La tipologia più comune di DTL è denominata "Blockchain", in riferimento al fatto che le transazioni sono raggruppate in blocchi uniti fra loro in ordine cronologico a formare una catena[32]. L'intera catena è protetta da complessi algoritmi matematici che hanno lo scopo di garantire l'integrità e la sicurezza dei dati in essa contenuti[33]. Questa catena forma il registro completo di tutte le transazioni incluse nel database.

Possiamo quindi affermare che le Blockchain sono delle *distributed ledger technologies*, consistenti in un registro distribuito strutturato in modo da gestire le transazioni all'interno di una catena di blocchi. Dal punto di vista strutturale, ciascun blocco si "aggiunge" alla catena sulla base di un processo fondato sul consenso distribuito su tutti i nodi della rete, ovvero con la partecipazione di tutti i nodi che vengono chiamati a contribuire alla validazione delle transazioni presenti in ciascun blocco e alla loro "inclusione" nel registro (vedi *paragrafo 2.1.3*)[34]. Le DLT, e quindi le Blockchain, prevedono infatti un meccanismo di validazione delle transazioni a sua volta distribuito: "*le modalità di gestione del consenso unitamente alle logiche di impostazione del registro rappresentano due fra i principali punti qualificanti della carta d'identità delle tecnologie distributed*

[32] D. LEE Kuo Chuen, R. H. DENG, "*Handbook of blockchain, digital finance and inclusion – volume 2",* Elsevier, 2018.
[33] Fonte: "*L'influenza dell'innovazione tecnologica in ambito finanziario*", Avv. Barbara Bandiera, 2018.
[34] Fonte: Rossana Morriello, "*Blockchain, intelligenza artificiale e internet delle cose in biblioteca*", 2019.

ledger"[35]. Ed è all'interno di questo insieme di tecnologie che trovano la loro collocazione le Blockchain.

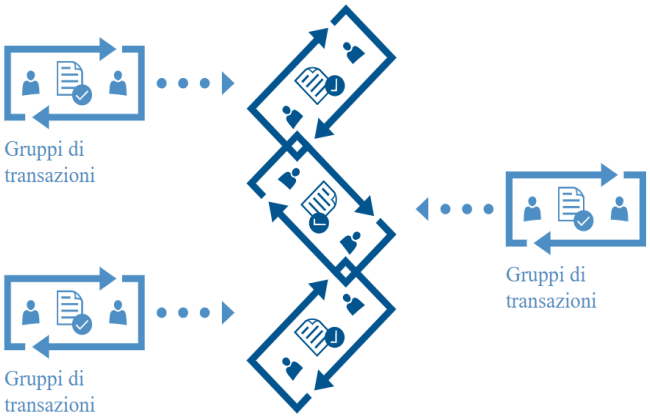

Figura 11. Blockchain come insieme di transazioni. Fonte: sito ufficiale Banca Centrale Europea.

2.1.2 La crittografia

Il tema della sicurezza della corrispondenza è antico quanto l'uomo, che da sempre ha cercato il modo di proteggere i suoi segreti e la sua vita privata.

I primi esempi di uso della crittografia si hanno addirittura dall'epoca dell'Impero romano, quando Giulio Cesare utilizzava il metodo della traslazione delle lettere dei messaggi che inviava, "scalando" cioè le lettere di 3 posizioni (la A diventava C, la B diventava D e così via). Dalle origini della crittografia chiaramente molte cose sono cambiate: oggi il suo significato si colloca nell'ambito della sicurezza

[35] Fonte: "*Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia*", Mauro Bellini, 2020.

informatica[36]. Attualmente, infatti, esistono parecchi algoritmi crittografici che utilizzano la grande potenza di calcolo dei moderni calcolatori elettronici, così come gli stessi sono impiegati nel tentativo di decifrare quello che è stato codificato da altri.

La crittografia, per definizione, è la branca della crittologia che tratta delle "scritture nascoste", ovvero dei metodi per rendere un messaggio "offuscato" in modo da non essere comprensibile e intelligibile a persone non autorizzate a leggerlo. In altre parole, è una tecnica che permette di "cifrare" un messaggio rendendolo incomprensibile a tutti fuorché al suo destinatario. Un testo realizzato secondo i principi della crittografia si dice "cifrato" e affinché sia riportato nella sua forma in chiaro il destinatario deve compiere una "decifrazione". La stessa operazione attuata da chi non è autorizzato a leggere il messaggio si chiama "decrittazione" e "crittanalisi" l'insieme delle teorie e delle tecniche che se ne occupano.

La crittografia, dunque, può essere definita come un sistema che, tramite l'utilizzo di un algoritmo matematico, agisce sulla sequenza di caratteri di un messaggio, trasformandola[37]. Tale trasformazione si basa sul valore di una chiave segreta,

[36] Fonte: "*La crittografia: quando nasce, come funziona e perché è alleata della sicurezza informatica*", Francesca Carli, 2020.

[37] I sistemi di cifratura possono operare per *trasposizione* (mescolando i caratteri di un messaggio in un ordine diverso), o per *sostituzione* (scambiando un carattere con un altro in accordo ad una regola specifica), o implementare entrambe le tecniche ("*cifratura composta*"). In linea di massima una cifratura composta è più sicura di una cifratura basata solo su sostituzione o su trasposizione.

ovvero il parametro dell'algoritmo di cifratura/decifratura. E proprio la segretezza di questa chiave rappresenta il sigillo di sicurezza di ogni sistema crittografico[38].

Fino a qualche anno fa il metodo crittografico *simmetrico* (o "a chiave segreta") era l'unico esistente: esso prevede l'utilizzo di un'unica chiave, sia per nascondere il messaggio che per renderlo nuovamente leggibile. Tuttavia si sono rilevati alcuni limiti connessi all'utilizzo di tali algoritmi, quali:

- Il necessario scambio della chiave segreta tra i due interlocutori coinvolti nell'operazione implica che una terza persona potrebbe impossessarsene durante la trasmissione;
- L'appropriazione della chiave da parte di una persona esterna alla transazione renderebbe visibile a quest'ultima tutto il "traffico" di informazioni scambiate e possibile l'alterazione dei messaggi originali senza che il destinatario se ne accorga;

La vera novità del secolo scorso, infatti, è legata all'invenzione della tecnica crittografica *asimmetrica* (o "a doppia chiave"), che utilizza due chiavi distinte (una pubblica ed una privata) per cifrare e per decifrare un messaggio. La coppia di chiavi è legata matematicamente da una funzione, che assicura che un

[38] Fonte: R. L. Rivest, A. Shamir, L. Adleman. "*A method for obtaining digital signatures and public-key cryptosystems*", 1978.

messaggio criptato con una delle due chiavi possa essere decifrato solo dall'altra[39].

L'esempio di seguito proposto ci aiuterà nella comprensione di quanto appena enunciato.

L'utente *A* decide di inviare un documento di testo all'utente *B*, ma vuole accertarsi del fatto che solo *B* sia in grado di leggere il contenuto di tale messaggio: *A* decide quindi di utilizzare la crittografia asimmetrica, servendosi della chiave pubblica di *B* (che, essendo pubblica, è stata messa pubblicamente a disposizione da *B*) per criptare il messaggio da inviare. Il documento così criptato non è più decifrabile da *A*, in quanto non è in possesso della chiave privata di *B* (che, essendo privata, è a sola disposizione di *B*). L'utente *B* riceve quindi il documento e riesce a decifrarlo utilizzando la sua chiave privata.

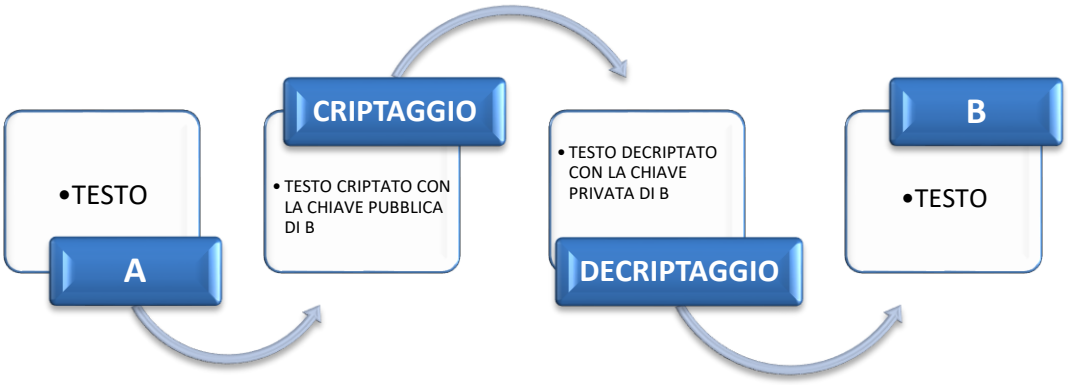

Figura 12. Esempio di crittografia asimmetrica. Fonte: elaborazione dell'autore.

[39] Fonte: "*A method for obtaining digital signatures and public-key cryptosystems*", R. L. Rivest, A. Shamir, L. Adleman, 1978.

Dall'esempio proposto è intuibile pertanto che chiunque sia in possesso della chiave pubblica usata per criptare un messaggio non sarà in grado di decifrarlo: l'unico modo per farlo è essere in possesso della chiave privata associata a quella pubblica utilizzata[40].

In realtà, esistono due distinte modalità di utilizzazione della tecnica crittografica "a doppia chiave":

- "*Public to private*": meccanismo secondo cui, come da esempio appena proposto, la chiave pubblica cripta e quella privata decripta (*figura 12*). Chiunque può creare un testo criptato ma solo il proprietario della chiave privata potrà decriptarlo.
- "*Private to public*": inverso rispetto al precedente, è quel meccanismo che permette esclusivamente al proprietario della chiave privata di criptare il messaggio, che può essere letto da tutti coloro che sono in possesso della chiave pubblica.

Inerentemente alla tecnologia Blockchain, è possibile affermare che questa utilizza la **crittografia "a doppia chiave"** per permettere lo scambio sicuro di beni (come ad esempio di criptovalute) tra una persona e l'altra. Ogni utente che detiene un bene sulla Blockchain, infatti, è in possesso di una chiave pubblica (nota anche come "*address*") e di una privata[41].

[40] Fonte: Marilù Pagano, "*Blockchain. Cyberwar e strumenti di intelligence*" 2017.
[41] Fonte: Bernasconi Anna, Ferragina Paolo, Luccio Fabrizio, "*Elementi di crittografia*", 2015.

Più nello specifico, BC utilizza l'approccio "*public to private*" per identificare i proprietari degli account e trasferire la proprietà tra gli stessi e quello "*private to public*" per autorizzare le transazioni.

Per rendere più semplice la comprensione del fenomeno faremo riferimento, in via esemplificativa, a due utenti in possesso di due chiavi pubbliche differenti:

- Enzo | *address*: 0x1234567890
- Stefano | *address*: 0x5678901234

Enzo e Stefano sono identificati all'interno della Blockchain con un *address* pubblico: chiunque voglia inviare loro dei beni dovrà farlo utilizzando il loro indirizzo[42]. Ognuno di loro, inoltre, è in possesso della rispettiva chiave privata: questa garantisce che l'invio di eventuali beni sia realmente voluto dal proprietario[43].

Proponiamo nel dettaglio il procedimento che avverrebbe se Enzo dovesse inviare 1 bitcoin (BTC) a Stefano: in primo luogo, Enzo accede ai suoi beni presenti in BC utilizzando la chiave privata in suo possesso, per poi trasferire 1 bitcoin verso l'*address 0x5678901234* di Stefano. La transazione, attraverso l'approccio crittografico "*private to public*", viene autorizzata da Enzo tramite la sua chiave privata e, poi, attraverso il meccanismo "*public to private*", criptata utilizzando la

[42] Fonte: Marilù Pagano, "*Blockchain. Cyberwar e strumenti di intelligence*" 2017.
[43] Di fatti, solo chi possiede la chiave privata è in grado di effettuare il trasferimento di un bene. Ovviamente, chiunque altro entri in possesso della stessa chiave sarà in grado di effettuare qualsiasi tipo di operazione in nome e per conto del proprietario (proprio come se conoscesse le credenziali per accedere al suo *on-banking*).

chiave pubblica di Stefano. A questo punto, solamente Stefano sarà in grado di decriptare la transazione, utilizzando, a sua volta, la chiave privata in suo possesso.

Figura 13. Transazione di 1 BTC in BC. Fonte: elaborazione dell'autore.

Comunemente, e in senso figurato, si dice che le criptovalute degli utenti siano conservate all'interno di appositi *wallet*, i quali tengono traccia di tutte le transazioni che avvengono all'interno della Blockchain[44]. L'utilità di un *wallet* è paragonabile a quella offerta da un comune conto corrente bancario, con la differenza che la Blockchain non richiede il codice fiscale o altri dati identificativi per aprirne e possederne uno. Quando viene aperto un *wallet*, al proprietario vengono fornite sia la chiave pubblica che quella privata[45]. Tramite la chiave

[44] Fonte: Joel Hartman, "*Cryptocurrency & Blockchain: how to generate passive income with your blockchain wallet*", 2019.
[45] Fonte: Joel Hartman, "*Cryptocurrency & Blockchain: how to generate passive income with your blockchain wallet*", 2019.

pubblica è possibile ricevere pagamenti (motivo per cui è resa "pubblica"), attraverso quella privata, invece, è possibile sbloccare il *wallet* ed effettuare qualsiasi operazione[46]. La chiave privata rappresenta di fatti la "firma digitale"[47] del proprietario del *wallet*, in grado di autorizzare qualsiasi tipo di transazione. Per fare un esempio, si potrebbe paragonare la chiave pubblica ad un bancomat e la chiave privata al suo pin: essendo la chiave pubblica (bancomat) nota a tutti, chiunque entrasse in possesso della chiave privata (pin) sarebbe in grado di spendere ed inviare fondi a qualsivoglia indirizzo, in nome e per conto del proprietario.

In via conclusiva, è lecito affermare che i trasferimenti tra due utenti all'interno di BC, come nel caso di Enzo e Stefano, avvengono "da chiave pubblica a chiave pubblica"[48]: una transazione di bitcoin non è nient'altro che il trasferimento di fondi dalla chiave pubblica di Enzo a quella di Stefano, in seguito all'apposizione della firma digitale (chiave privata) da parte di Enzo per autorizzare il trasferimento di denaro nei confronti di Stefano.

[46] Fonte: Bernasconi *et al*., 2015.
[47] Una "firma digitale" (dall'inglese "*digital signature*") è uno schema matematico per dimostrare l'autenticità di un messaggio/documento. Fonte: D. LEE Kuo Chuen, R. H. DENG, "*Handbook of blockchain, digital finance and inclusion – volume 2*", Elsevier, 2018.
[48] Fonte: Bernasconi *et al*., 2015.

2.1.3 Il mining e il consenso: cosa accade dietro alle quinte di una Blockchain

Il consenso è un meccanismo automatico che definisce una conoscenza comune delle regole, del controllo e del funzionamento di un network tra i suoi partecipanti[49]: non dimentichiamo, infatti, che nel caso di Blockchain siamo in presenza di una rete *peer-to-peer*, che, per definizione, non ammette la possibilità che un nodo eserciti il proprio controllo sugli altri[50].

Concordare sullo stato della Blockchain è essenziale per il corretto funzionamento di un sistema privo di un'autorità centrale preposta al controllo[51]. Pertanto, gli algoritmi di consenso costituiscono un elemento cruciale per ogni network distribuito, in quanto hanno il compito di mantenerne l'integrità e la sicurezza. Il più famoso tra questi è il *Proof-of-Work* (PoW), creato da Satoshi Nakamoto e implementato per la prima volta su Bitcoin. "*L'algoritmo PoW, nella fattispecie, consente ai partecipanti di una Blockchain di convalidare un nuovo blocco e aggiungerlo alla catena solo se i nodi del network raggiungono il consenso*"[52] concordando, quindi, sulla validità delle transazioni avvenute: tale algoritmo costituisce pertanto una parte essenziale del *mining process*.

[49] Fonte: "*Blockchain: che cos'è e come si potrebbe utilizzare*", Nicola Paoli, 2017.
[50] Fonte: Massimiliano Nicotra, Fulvio Sarzana di S. Ippolito, "*Diritto della blockchain, intelligenza artificiale e IoT*", 2018.
[51] Fonte: Maria Letizia Perugini, "*Distributed ledger technologies e sistemi di Blockchain: digital currency, smart contract e altre applicazioni*", 2018.
[52] Fonte: "*Crypto & Blockchain Education*", Binance Academy, 2020.

In questo paragrafo approfondiremo il processo di *mining* prendendo in esame, in via esemplificativa, la Blockchain di Bitcoin[53].

Il *mining*, che significa letteralmente "estrazione", è l'attività che consente di creare nuovi bitcoin, nonché di certificare, e quindi validare, le transazioni all'interno di una Blockchain. Come precedentemente accennato, ogni transazione che ha luogo in BC viene inserita all'interno di un blocco, che, prima di essere aggiunto alla catena dei blocchi precedenti, necessita di essere verificato, così da controllare che non vi siano errori che potrebbero compromettere le informazioni archiviate. Il processo di verifica delle transazioni avvenute e, quindi, l'accettazione di queste da parte della rete, viene svolto dai cosiddetti *miner*[54]: definiti come "nodi validatori", sono coloro che mettono a disposizione della rete la potenza di calcolo del proprio computer, al fine di validare le transazioni nella Blockchain. In linea generale, i *miner* hanno l'obiettivo di trovare un determinato valore che, aggiunto ad altri dati presenti nel blocco, restituisca un determinato codice *hash*[55]. Una volta che un *miner* trova la soluzione per validare il blocco, tutti gli altri nodi dovranno confermare la correttezza del risultato ottenuto e, in

[53] Bitcoin è, per l'appunto, una Blockchain che si basa su protocolli *Proof-of-Work*. Fonte: www.bitcoin.org.
[54] Fonte: Maria Letizia Perugini, "*Distributed ledger technologies e sistemi di Blockchain: digital currency, smart contract e altre applicazioni*", 2018.
[55] Un *hash*, per definizione, è una funzione non invertibile che converte una stringa di lunghezza arbitraria in una stringa finale di lunghezza predefinita (la quale prende appunto il nome di *hash*).

caso affermativo, il *miner* validatore otterrà la sua ricompensa in bitcoin[56]: da qui la creazione di nuovi bitcoin attraverso il processo di *mining*. In via definitiva, infine, il blocco verrà aggiunto alla catena, aumentandone la lunghezza.

L'intero processo descritto prende il nome di "*mining*" perché viene paragonato a quanto accade nelle miniere con gli estrattori d'oro: i *miner* consentono di fatti "l'estrazione", e quindi la creazione, di nuovi bitcoin[57].

Prima di proseguire nella trattazione e, in particolare, nella spiegazione delle modalità con cui i *miner* diventano artefici della validazione delle transazioni in BC, occorrono alcune delucidazioni relative al concetto di *hash*, precedentemente menzionato.

L'*hash* è una vera e propria "impronta digitale": si ricava partendo da più dati (input) di lunghezza, dimensione e formato variabile, che vengono processati tramite una "funzione di *hash*", che restituisce come output un codice (*hash*) di lunghezza predefinita[58]. Dal risultato ottenuto tramite l'output (cioè dall'*hash*) non è possibile risalire all'input (ovvero ai dati utilizzati per generarlo).

---

[56] Ovviamente, i nodi validatori vengono remunerati per svolgere questo processo di verifica e, di conseguenza, competono fra loro per risolvere il blocco: il primo che è in grado di risolverlo otterrà una ricompensa in bitcoin. Fonte: Joel Hartman, "*Cryptocurrency & Blockchain: how to generate passive income with your blockchain wallet*", 2019.

[57] Fonte: Joel Hartman, "*Cryptocurrency & Blockchain: how to generate passive income with your blockchain wallet*", 2019.

[58] Di qualsiasi dimensione siano i dati inseriti nell'input, l'*hash* ottenuto avrà la stessa lunghezza, definita dal tipo di funzione *hash* utilizzata. Fonte: Fonte: "*On the Secure Hash Algorithm family*", Wouter Penard, Tim Van Werkhoven, 2002.

È importante sottolineare che quando si applica la funzione di *hash* ad una parola o ad un testo si ottiene come risultato una sequenza di caratteri e di numeri di lunghezza predefinita: qualsiasi sia la dimensione e la complessità dell'input, l'*hash* corrispondente avrà sempre la stessa lunghezza[59] (*figura 14*).

Inoltre, un determinato *hash* corrisponderà sempre allo stesso input dal quale è stato generato[60]. Se, per esempio, dieci persone utilizzassero la funzione di *hash* sulla frase "Ciao come stai?", queste otterrebbero tutte lo stesso risultato, sia oggi che tra un anno. Allo stesso modo, se si cambiasse anche una sola lettera o si aggiungesse una virgola all'input, la funzione di *hash* restituirebbe risultati completamente differenti (*figura 14*).

[59] Fonte: "*On the Secure Hash Algorithm family*", Wouter Penard, Tim Van Werkhoven, 2002.
[60] Fonte: Penard *et al*., 2002.

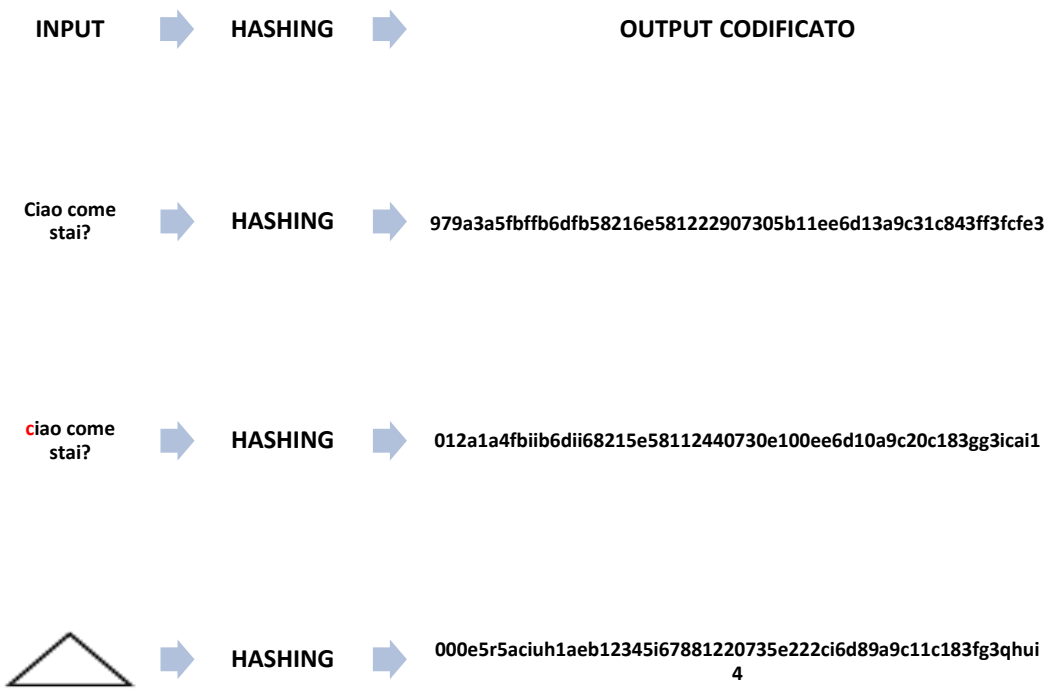

Figura 14. Funzione di hash. Fonte: elaborazione dell'autore.

Come già accennato, ai fini del processo di validazione di un blocco, i *miner* sono tenuti a risolvere un "rompicapo": nello specifico, essi devono trovare un numero chiamato *nonce*[61]. Questo, se processato tramite la funzione di *hash* insieme ad

[61] In crittografia il termine "*nonce*" indica un numero, generalmente casuale, che possiede un utilizzo unico. Tale termine deriva infatti dall'espressione inglese "*number used once*", che significa appunto numero usato una sola volta. Fonte: "*On the Secure Hash Algorithm family*", Wouter Penard, Tim Van Werkhoven, 2002.

altri dati presenti nel blocco da validare[62], deve restituire un *hash* che inizi con un determinato numero di zeri[63], chiamato "*hash* della testa del blocco".

È opportuno precisare che non esiste una tecnica o un calcolo per trovare un *nonce* valido: l'unico modo logico per farlo è tramite numerosi tentativi casuali. Proprio per questo motivo i nodi validatori si servono di appositi hardware che misurano la loro potenza in "tentativi al secondo" (H/s)[64]. Da qui nasce il concetto di "competizione tra *miner*": solo il *miner* che troverà per primo un *nonce* valido, infatti, verrà ricompensato per il lavoro svolto. Egli, una volta trovata la soluzione, dovrà comunicarla agli altri nodi della rete, che effettueranno a loro volta una verifica per confermare che il *nonce* sia effettivamente valido.

Un esempio ci aiuterà nella comprensione del processo appena descritto.

Supponiamo che il grado di difficoltà per la validazione di un blocco sia di 7 zeri.

I *miner* competeranno tra loro per trovare un *nonce* valido: quest'ultimo, se processato insieme agli altri dati presenti nella testa del blocco, deve restituire un codice *hash* che presenta, nel caso specifico, 7 zeri iniziali. L' "*hash* della testa del blocco" generato avrà pertanto le caratteristiche del seguente:

- **0000000**h3ie95……

[62] Ogni blocco contiene, oltre alle transazioni, dei dati allocati nella "testa" del blocco stesso.
[63] Il numero di zeri è definito in uno dei dati presenti nella testa del blocco e definisce il grado di difficoltà per la validazione del blocco: maggiore è il numero di zeri presenti e maggiore sarà la difficoltà di validazione per il *miner*. Fonte: Joel Hartman, "*Cryptocurrency & Blockchain: how to generate passive income with your blockchain wallet*", 2019.
[64] Fonte: Penard *et al*., 2002.

Una volta trovata la soluzione, il *miner* validatore fornirà il risultato agli altri nodi della rete per provare la validità del lavoro svolto. Se corretto, il blocco sarà validato ufficialmente e "attaccato" alla catena di blocchi precedenti e il nodo validatore verrà ricompensato con l'immissione di nuovi bitcoin.

Il tempo necessario per la validazione di un blocco dipende puramente dal grado di difficoltà impostato per la ricerca del *nonce*[65]. Possiamo affermare che, in media, la verifica e la validazione di un blocco nella Blockchain di Bitcoin avviene ogni 10 minuti[66]. Questa tempistica non è casuale: l'algoritmo Bitcoin è stato programmato per fare in modo che, ogni due settimane, il grado di difficoltà per la validazione di un blocco venga adattato alla potenza di calcolo di tutti i nodi preposti all'attività di *mining*: maggiore è la potenza di calcolo totale, più verrà aumentata la "difficoltà di *mining*", così da mantenere la media di 10 minuti per la validazione di ogni blocco. Mantenere queste tempistiche di validazione è importante per la politica monetaria di Bitcoin, in quanto il processo di *mining* rappresenta l'unico modo con cui nuovi bitcoin vengono messi in circolazione[67].

In via conclusiva, riprendendo l'esempio di Enzo e Stefano proposto nel precedente paragrafo, offriamo di seguito un'immagine riassuntiva del processo che si aziona dal momento in cui viene inviata una transazione nella Blockchain di Bitcoin fino alla validazione del blocco da parte dei *miner*:

---

[65] Fonte: Penard *et al*., 2002.
[66] Fonte: www.bitcoin.org.
[67] Tale meccanismo fa sì che non esista nessun metodo per immettere in rete nuovi bitcoin più velocemente. Fonte: www.bitcoin.org.

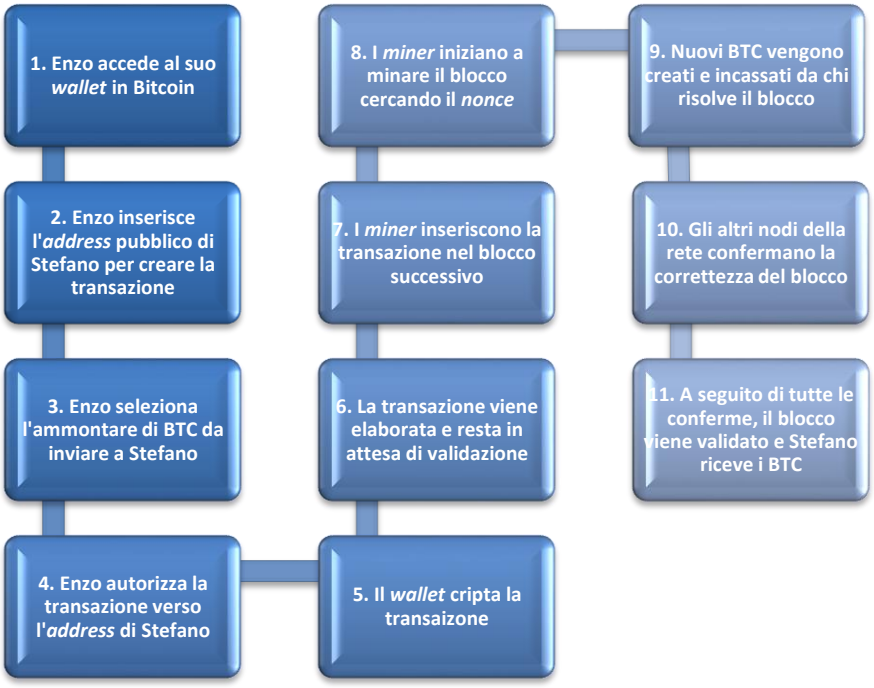

Figura 15. Il percorso di una transazione in BC. Fonte: elaborazione dell'autore.

A questo punto della trattazione, si rende necessario approfondire il meccanismo secondo il quale la maggioranza dei nodi della rete "elegge" la versione corretta della Blockchain, qualora dovesse pervenirne più di una.

Tale meccanismo, definito "*Distributed Consensus*"[68], consente a tutti i partecipanti del network di selezionare a maggioranza un'unica e corretta versione della catena da approvare. La selezione si basa su due criteri principali:

[68] Meccanismo tramite cui gli utenti all'interno di un network P2P concordano sulla validità dei dati contenuti nel libro mastro. Fonte: "*Distributed Ledger Technology & Cybersecurity: Improving information security in the financial sector*" Enisa, 2016.

- Criterio della catena più lunga: si fonda sull'idea che la struttura di dati della Blockchain che comprende il maggior numero di blocchi sia quella che rappresenta il maggior sforzo computazionale e sia da ritenersi, quindi, quella corretta[69].
- Criterio della catena più "pesante": nel momento in cui più catene di blocchi fossero di uguale lunghezza, i nodi si baserebbero sull'idea secondo la quale la catena che è stata costruita utilizzando la maggior difficoltà di calcolo in aggregato rappresenti il maggior sforzo computazionale e sia da ritenersi, quindi, quella corretta.

I criteri descritti fanno desumere una delle assunzioni fondamentali della tecnologia Blockchain: fino a quando i nodi onesti mantengono la maggioranza della potenza computazionale di tutto il sistema (51%), la catena mantenuta dagli stessi tenderà a crescere più velocemente rispetto a tutte le altre catene alternativamente proposte[70]. Allo stesso modo, se un gruppo di *miner* disonesti riuscisse a prendere possesso del 51% della rete di validatori, non sarebbero più i partecipanti onesti a decidere arbitrariamente la veridicità o meno delle transazioni processate, bensì quelli disonesti. Tale fattispecie è da sempre considerata, a ben vedere, uno dei più grandi pericoli del sistema Blockchain. Ma

[69] Fonte: Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S., "B*itcoin and cryptocurrency technologies: A comprehensive introduction*", Princeton University Press, 2016.
[70] Prove empiriche dimostrano che i *miner* si comportano in modo strategico e formano delle vere e proprie organizzazioni, definite "*Pool*", che agiscono come un'unica entità: la forza di un *Pool* è la somma della potenza computazionale dei suoi membri. Fonte: Joel Hartman, "*Cryptocurrency & Blockchain: how to generate passive income with your blockchain wallet*", 2019.

numerosi studi hanno rilevato che a nessun gruppo di *miner* converrebbe comportarsi in maniera disonesta, poiché ciò causerebbe un crollo della fiducia nei confronti del sistema stesso, provocando la fuga di tutti i partecipanti onesti dalla rete e comportando, di conseguenza, un danno ai disonesti stessi[71].

2.1.4 La gestione dei dati

La gestione dei dati all'interno della Blockchain, come più volte sottolineato, avviene attraverso l'utilizzo di una catena di blocchi condivisa tra i partecipanti del network.

In riferimento a quanto finora spiegato, appare opportuno specificare che ogni blocco contiene al suo interno, oltre ad una serie di dati concernenti le **transazioni** avvenute in rete, dei parametri fondamentali per l'identità del blocco stesso: il ***time-stamp*** della sua creazione e il **riferimento al blocco immediatamente precedente**[72].

Se l'autorevolezza delle operazioni in BC si ottiene tramite la validazione dei blocchi da parte degli utenti della rete, la sicurezza si raggiunge, invece, come accade di norma nel mondo digitale, certificando l'avvenuta autorizzazione delle

[71] Fonte: "*Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack*", Sarwar Sayeed, Hector Marco-Gisbert , University of the West of Scotland, 2019.
[72] Fonte: "*Decentralized Trusted Timestamping using the Crypto Currency Bitcoin*", Bela Gipp, Norman Meuschke, André Gernandt, 2015.

operazioni in un determinato istante temporale[73]. Nello specifico, all'interno della struttura Blockchain questa certificazione prende il nome di "*timestamping*", operazione in grado di generare in output una sequenza di caratteri specifici tramite cui si indica in modo univoco e immutabile la data e/o l'orario di accadimento di ogni operazione[74]. Il *timestamping* allora permette, assieme al meccanismo di consenso distribuito alla base di ogni Blockchain (*paragrafo 2.1.3*), di garantire la sicurezza di ogni transazione.

Una volta che tutte le operazioni vengono opportunamente "timbrate" tramite marca temporale, e quindi inserite all'interno del blocco, quest'ultimo dovrà essere chiuso e "certificato": verrà cioè processato in qualità di input attraverso un algoritmo di *hashing*, che genererà un "messaggio in codice" esclusivo ed identificativo del blocco stesso[75] (*figura 16*).

[73] Fonte: Massimiliano Nicotra, Fulvio Sarzana di S. Ippolito, "*Diritto della blockchain, intelligenza artificiale e IoT*", 2018.
[74] Fonte: D. LEE Kuo Chuen, R. H. DENG *"Handbook of blockchain, digital finance and inclusion – volume 2*", Elsevier, 2018.
[75] Fonte: *"Blockchain: che cos'è e come si potrebbe utilizzare*", Nicola Paoli, 2017.

Figura 16. Creazione del codice hash in riferimento al Blocco 1. Fonte: "Blockchain: che cos'è e come si potrebbe utilizzare", Nicola Paoli, 2017.

Blockchain salverà il codice *hash* generato, in qualità di parametro identificativo, all'interno del blocco stesso: in tal modo il blocco risulterà certificato, ovvero chiuso e immodificabile[76] (*figura 17*).

Figura 17. Certificazione del Blocco 1. Fonte: "Blockchain: che cos'è e come si potrebbe utilizzare", Nicola Paoli, 2017.

[76] Fonte: *"Blockchain: che cos'è e come si potrebbe utilizzare*", Nicola Paoli, 2017.

Quando si genererà un secondo blocco, oltre alle transazioni, al *time-stamp* della sua creazione e al codice *hash* identificativo, sarà necessario includere al suo interno anche il codice *hash* identificativo del blocco precedente[77]: ogni blocco della catena, pertanto, conterrà un riferimento al blocco immediatamente precedente (*figura 18*). Con tale meccanismo Blockchain fa in modo che tutti i blocchi siano inequivocabilmente collegati tra loro: qualsiasi modifica all'interno di un blocco invaliderà, oltre al blocco stesso, l'intera catena[78].

Figura 18. Collegamento tra tutti i blocchi della catena. Fonte: "Blockchain: che cos'è e come si potrebbe utilizzare", Nicola Paoli, 2017.

In via conclusiva, possiamo affermare che la gestione dei dati all'interno della Blockchain avviene in maniera *append-only*, permettendo cioè ai partecipanti del

[77] Fonte: A. Back et Al., "*HashCash*", 2002.
[78] Fonte: *"Blockchain: che cos'è e come si potrebbe utilizzare*", Nicola Paoli, 2017.

network unicamente di aggiungere dati ed informazioni all'interno della piattaforma, escludendo la possibilità di eliminare o manipolare i dati esistenti.

2.1.5 The Double Spending problem

La tecnologia Blockchain, come più volte sottolineato, è stata resa pubblicamente nota nell'inverno del 2008 per opera del suo ideatore, Satoshi Nakamoto, attraverso il *white paper* dal titolo "*Bitcoin: A Peer-to-Peer Electronic Cash System*", tramite cui il mondo è venuto a conoscenza di una delle Blockchain ad oggi più note, il sistema Bitcoin. L'obiettivo del *paper* fu quello di illustrare come Bitcoin potesse permettere trasferimenti digitali di denaro tra utenti senza la necessità di coinvolgere una terza parte con la funzione di intermediario delle transazioni[79]. L'approvazione e l'interesse maturati nei confronti del sistema verrebbero però a mancare, secondo Nakamoto, nel momento in cui il sistema stesso non riesca a garantire, oltre alla velocità e all'immediatezza delle transazioni, la loro autenticità e sicurezza[80].

Negli odierni sistemi economici, il trasferimento digitale di *asset*, come ben sappiamo, non può avvenire senza la presenza di un ente regolatore, che si pone come garante dell'autenticità e della sicurezza delle transazioni tra utenti. Si pensi, a tal proposito, alla funzione svolta dalle banche: se si vuole eseguire una

[79] Fonte: Nakamoto, "*Bitcoin: A Peer-to-Peer Electronic Cash System*", 2008.
[80] Fonte: Nakamoto, 2008.

transazione online (ad esempio un bonifico), l'operazione può avvenire solamente attraverso la piattaforma digitale dell'istituto di credito e a fronte, nella maggior parte dei casi, del pagamento di un onere. Il ruolo della banca, propriamente, è quello di autorizzare la transazione, verificando che la somma di denaro che viene trasferita da un utente sia compatibile con le disponibilità del suo conto corrente, procedendo quindi con la riduzione dell'ammontare depositato dal primo correntista di una somma pari a quella trasferita e incrementando il conto del beneficiario della stessa somma. In sintesi, ciò di cui la banca si fa garante è evitare il verificarsi di una situazione che in letteratura viene definita "*Double Spending*".

Il problema della duplicazione è insisto nel mondo digitale, in cui il passaggio di *asset* implica automaticamente la duplicazione degli stessi. Si pensi per esempio ad un documento di testo scritto in Word: nel momento in cui questo viene trasferito da un utente ad un altro ne viene creata immediatamente una copia e il possesso di quel documento sarà condiviso dai due utenti, ciascuno dei quali sarà libero di trasferirlo nuovamente ad altri[81].

Ma se la duplicazione di un generico documento non comporta particolari problematiche, quella di un *asset* progettato per rappresentare una valuta in

[81] Fonte: "*Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia*", Mauro Bellini, 2020.

digitale provocherebbe una diminuzione progressiva del suo valore[82]: ecco perché il mondo della finanza, prima di tutti, ha compreso l'importanza della Blockchain relativamente alla sua capacità di garantire l'unicità di un *asset* digitale. Infatti, l'avvento della Blockchain consente di far "riconquistare" al mondo digitale il concetto di "scarsità dei beni" del mondo reale: nel momento in cui trasferiamo un *asset* digitale tramite la BC, quel bene conserverà la sua unicità[83].

In sintesi, la proposta di Nakamoto fu proprio quella di introdurre una tecnologia (la Blockchain) che fosse in grado di consentire il trasferimento di *asset* tra utenti senza la necessità di coinvolgere una terza parte intermediaria, escludendo al tempo stesso la possibilità di duplicare l'oggetto della transazione[84]. Con l'intuizione di Nakamoto si è pertanto definita una soluzione al problema del *Double Spending*: la BC garantisce infatti che uno stesso *asset* monetario non sia utilizzabile più di una volta dal medesimo acquirente. Questa proprietà può essere definita come la capacità della Blockchain di creare e mantenere *asset* digitali unici, caratteristica rivoluzionaria che ne ha decretato il successo[85].

[82] Fonte: Chohan, Usman W., "*The Double Spending Problem and Cryptocurrencies*", 2017.
[83] Fonte: Massimiliano Nicotra, Fulvio Sarzana di S. Ippolito, "*Diritto della blockchain, intelligenza artificiale e IoT*", 2018.
[84] Fonte: Chohan *et al*., 2017.
[85] Fonte: www.blockchain.com.

2.1.6 Le varie tipologie di Blockchain

La Blockchain di Bitcoin, così come quella delle altre criptovalute, si presenta, come già affermato, come un libro mastro di transazioni raggruppate in blocchi distribuiti in una rete "libera"[86] di nodi paritari. Questa tipologia di Blockchain prende il nome di *Permissionless*, poiché non prevede il bisogno di generare autorizzazioni affinché gli utenti possano partecipare al controllo e alla validazione delle transazioni[87]. Nessun utente, infatti, può in alcun modo impedire che un'operazione venga inserita nel *ledger* una volta che è stata approvata da tutti i nodi della rete. Questo modello di Blockchain risulta pertanto adeguato per l'esecuzione di tutti quei documenti di cui va garantita l'assoluta immutabilità nel tempo.

Ma esiste un'altra tipologia di Blockchain, definita *Permissioned*, utilizzata per scambiare informazioni in maniera privata. Le *Permissioned* sono quelle Blockchain che possono essere controllate e quindi sottoposte ad una sorta di "proprietà". Il sistema di approvazione e inserimento/modifica di una transazione nel *ledger*, infatti, non è vincolato all'approvazione da parte di tutti i nodi della rete ma ad un numero limitato di utenti che sono definiti come *trusted*[88]. Il modello *Permissioned* è il tipo di Blockchain più adeguato per istituzioni o grandi

[86] Da riferirsi come "senza barriere all'ingresso".
[87] Fonte: "*Network Layer Aspects of Permissionless Blockchains*", Till Neudecker, Hannes Hartenstein, 2019.
[88] Fonte: Michele Faioli, Emanuele Petrilli, Donato Faioli, "*Blockchain, contratti e lavoro. La ri-rivoluzione digitale nel mondo produttivo e nelle PA*", 2019.

realtà aziendali che, dovendo intrecciare relazioni con diversi attori (fornitori, clienti, etc.), necessitano che le operazioni svolte siano soggette al controllo dei soli che ne abbiano l'autorizzazione. Di fatti, tali modelli fanno affidamento su un ristretto gruppo di utenti a cui viene permessa la validazione delle transazioni in funzione della fiducia di cui sono investiti[89]. Tali sistemi, per funzionare correttamente, devono quindi poter contare su una rete privata, chiusa e affidabile, la cui sicurezza è legata alla sua impenetrabilità da parte dei soggetti esterni.

Oltre a differenziarsi per il fatto che permettono o meno agli utenti la validazione e la certificazione dei dati presenti sulla rete, le Blockchain possono essere raggruppate sotto un'altra classificazione, distinguendole cioè tra pubbliche e private. Il modello pubblico (o "purista"), che vede la sua massima applicazione nella Blockchain di Bitcoin, prevede che l'accesso al network sia consentito a chiunque voglia partecipare e che abbia strutture necessarie e sufficienti in termini di software e capacità di elaborazione dei dati[90]. Le Blockchain private, invece, prevedono che l'accesso al network sia garantito ai soli partecipanti che ne hanno diritto[91].

[89] Fonte: Faioli *et al.*, 2019.
[90] Fonte: : Michele Faioli, Emanuele Petrilli, Donato Faioli, "*Blockchain, contratti e lavoro. La ri-rivoluzione digitale nel mondo produttivo e nelle PA*", 2019.
[91] Fonte: Faioli *et al.*, 2019.

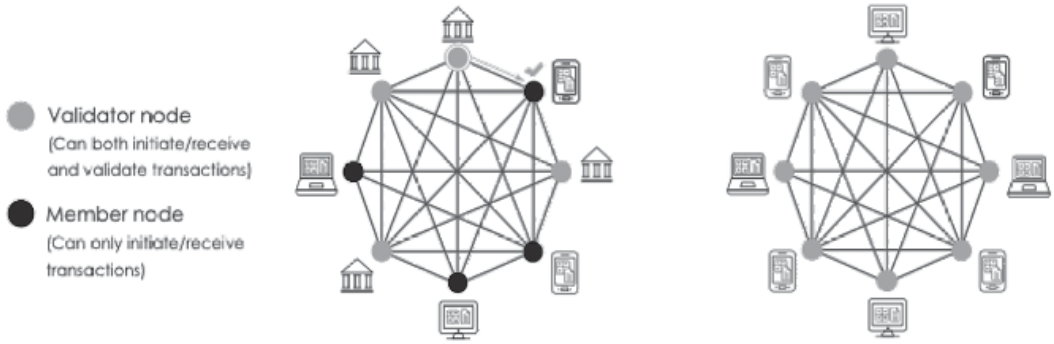

Figura 19. Tipologie di Blockchain distinte in base alla tipologia di controllo e alla tipologia di accesso. Fonte: Michele Faioli, Emanuele Petrilli, Donato Faioli, "Blockchain, contratti e lavoro. La ri-rivoluzione digitale nel mondo produttivo e nelle PA", 2019.

2.1.7 Vantaggi della Blockchain

Dopo aver descritto la struttura tecnologica della Blockchain in tutte le sue parti, procediamo a riassumerne, in via conclusiva, le principali caratteristiche, che sono anche i vantaggi che la valorizzano[92]:

- **DIGITALITÀ**

  La Blockchain permette, in svariati ambiti applicativi, di utilizzare il canale digitale come principale sistema di trasmissione di informazioni ed esecuzione di transazioni di diversa tipologia.

- **AFFIDABILITÀ E SICUREZZA**

[92] Fonte: Jason Griffey, "*The what, how, and why of blockchain for libraries*", 2016.

L’affidabilità della Blockchain è dovuta alla logica decentralizzata e distribuita su cui tale struttura si fonda: il consenso e la validazione dei dati e delle informazioni contenute in BC è affidato ai partecipanti stessi della rete.

- **TRASPARENZA**

  Tutti i nodi della rete possono prendere visione, in egual modo, di ogni informazione presente in Blockchain: non esistono posizioni di privilegio di alcuni nodi su altri, in particolar modo nella sua versione pubblica.

- **IMMUTABILITÀ**

  La caratteristica dell’immutabilità si riferisce all’abilità delle Blockchain di prevenire l’alterazione di transazioni che sono già state confermate: nessuno può alterare o modificare le informazioni contenute nel registro una volta inserite ed approvate, così come nessun nodo può inserirne di nuove senza l’approvazione di tutti gli altri partecipanti della rete.

- **INDIPENDENZA**

  La Blockchain è indipendente poiché elimina la necessità di individuare una terza parte con il ruolo di *supervisor* delle operazioni che vengono effettuate dagli utenti di tutto il mondo.

Figura 20. Principali vantaggi della Blockchain. Fonte: elaborazione dell'autore.

CAPITOLO 3

BLOCKCHAIN NEL BUSINESS

Un *business network* può esser generalmente definito come un insieme di relazioni tra imprese connesse[93] o, in alternativa, come un insieme di reti commerciali in cui avvengono scambi di beni e servizi tra diverse aziende[94]. E ogni transazione, appunto, viene generata dallo scambio di uno o più beni (o *asset*). Ciascun partecipante del network deve tracciare e registrare tutte le transazioni avvenute, per questioni legali o semplicemente per effettuare analisi di business e di mercato. Tali dati saranno poi necessariamente messi a disposizione degli organi regolatori che hanno la finalità di svolgere funzioni di controllo, verifica e regolamentazione di mercato.

Il meccanismo appena descritto presenta, però, alcuni limiti infrastrutturali. Innanzitutto è un sistema inefficiente, poiché ogni azienda si deve occupare autonomamente della verifica, della protezione e dell'aggiornamento dei propri dati; in più, per ogni transazione ci sono almeno due organizzazioni che tracciano esattamente le stesse informazioni. In secondo luogo, è anche un sistema

[93] Fonte: James C. Anderson, Håkan Håkansson, Jan Johanson, "*Dyadic Business Relationships within a Business Network Context*", Journal of Marketing, 1994.
[94] Fonte: Astley e Fombrun, 1983; Miles e Snow, 1992.

dispendioso: verificare la corrispondenza dei dati nei diversi registri continua a richiedere tempi molto lunghi e, ovviamente, costi elevati. Infine, risulta essere un sistema vulnerabile: i dati, infatti, risiedendo sui database delle singole aziende, possono essere affetti sia da banali errori di modifica o cancellazione sia da eventuali frodi o contraffazioni, molto difficili da identificare e da limitare.

Ed è per superare tali limiti che si rende necessario introdurre nel contesto business i concetti emersi con la Blockchain, approfonditi nel corso del capitolo precedente.

Innanzitutto, l'architettura distribuita di Blockchain permette di mettere in contatto tutti gli attori business appartenenti al network in modo diretto, senza intermediari. In secondo luogo, ogni nodo della rete possiede un database contenente una copia aggiornata degli stessi dati, che restano quindi continuamente sincronizzati all'interno del sistema in modo automatico[95]: i dati verificati vengono dapprima salvati in blocchi concatenati persistenti e poi sincronizzati fra tutti i nodi del network (*cap. 2, par. 2.1.1*). L'utilizzo della crittografia e dei permessi, inoltre, permette alle aziende di limitare la consultazione dei dati *(cap. 2, par. 2.1.2*), garantendo, ad esempio, l'accesso a determinate aziende selezionate, oppure creando canali di comunicazione esclusivi tra alcune aziende della stessa rete. Tutto ciò viene poi regolato in modo

[95] Fonte: Massimiliano Nicotra, Fulvio Sarzana di S. Ippolito, "*Diritto della blockchain, intelligenza artificiale e IoT*", 2018.

trasparente ed automatico mediante il "consenso", meccanismo automatico che definisce una conoscenza comune delle regole, del controllo e del funzionamento del network tra i suoi partecipanti[96] (*cap. 2, par. 2.1.3*).

È intuibile, a seguito di tali considerazioni, che i benefici apportati dalla Blockchain nel business sono molteplici:

- ⇨ **Risparmio di tempo**, per tutto ciò che riguarda l'aspetto burocratico (verifiche, autorizzazioni, controlli, licenze, etc.);
- ⇨ **Riduzione dei costi** relativi a tutte le operazioni coinvolte (costi per la verifica dei dati, costi di mantenimento, protezione e controllo delle informazioni aziendali, e così via),
- ⇨ **Diminuzione del rischio** di errori o frodi nella gestione dei dati: il concetto di persistenza e robustezza della catena e, quindi, l'impossibilità di apportare al sistema modifiche non autorizzate riduce notevolmente il rischio di compromissione della rete;
- ⇨ **Creazione di nuove opportunità** di mercato, ammettendo per qualsiasi azienda la possibilità di contattare direttamente nuovi partener senza servirsi di intermediari.

[96] Fonte: "*Blockchain: che cos'è e come si potrebbe utilizzare*", Nicola Paoli, 2017.

3.1 Blockchain e smart contract

La Blockchain è una *trustless technology*[97], e ciò significa che, con o senza intervento delle regole di un ordinamento statale, e dunque al di là delle regole codicistiche, esiste un sistema privatistico transnazionale che, avendo permesso il download di un determinato dato in forma informatica-digitale, lo rende veritiero per tutti gli operatori, sempre monitorabile, immodificabile, senza che vi sia il contributo o il controllo da parte di una autorità pubblica terza[98]. Sulla Blockchain possono muoversi dati, valori e diritti mediante gli *smart contract*.

Secondo un parziale iniziale glossario, gli *smart contract* sono contratti intelligenti perché auto-definiscono il proprio contenuto, sulla base dell'oggetto e delle cause disposti dalle parti[99]. Metaforicamente, la Blockchain è il binario e gli *smart contracts* sono i vagoni su cui circolano beni e servizi previsti da tali contratti.

Si comprende, date queste definizioni, che introdurre la tecnologia Blockchain nel business determina, da una parte, la revisione delle regole interne al mercato, e, dall'altra, la revisione di quelle regole relative alla gestione interna alla medesima azienda[100].

---

[97] Fonte: Nakamoto, 2009.
[98] Fonte: Michele Faioli, Emanuele Petrilli, Donato Faioli, "*Blockchain, contratti e lavoro. La ri-rivoluzione digitale nel mondo produttivo e nelle PA*", 2019.
[99] Fonte: Nick Szabo, 1994: "*I call these new contracts smart, because they are far more functional than their inanimate paper-based ancestors. No use of artificial intelligence is implied*".
[100] Fonte: Michele Faioli, Emanuele Petrilli, Donato Faioli, "*Blockchain, contratti e lavoro. La ri-rivoluzione digitale nel mondo produttivo e nelle PA*", 2019.

La tecnologia Blockchain, per gli aspetti economici, è in grado di rivoluzionare il rapporto tra pubblico e privato perché è materia di politica industriale, di investimenti economici, di modernizzazione di un paese e di competizione[101].

Per l'organizzazione aziendale, in egual modo, è da intendersi come una rivoluzione perché incide sul modo mediante cui si rendono servizi e si produce.

Da un punto di vista giuridico, inoltre, "*è un fattore endogeno, non determinabile, non assolutizzabile, non valutabile in toto oggi, ma certamente già incisivo per l'organizzazione dei rapporti commerciali, dei rapporti tra PA e cittadino-utente, dei rapporti di lavoro*"[102].

Blockchain è, dunque, pura disintermediazione perché, essendo una tecnologia crittografica, rende giuridicamente possibile il trasferimento digitale di dati, valori, diritti e informazioni senza la presenza di terzi certificatori. È, in altre parole, una partita "tripla" (non più "doppia"), di livello globale, che permette di svolgere operazioni commerciali senza l'intervento di un terzo certificatore, con una rendicontazione crittografica che è verificata contestualmente dalla rete degli operatori, con una ricognizione storica delle vicende giuridiche che attengono a quel bene/servizio/diritto e con un continuo monitoraggio dell'adempimento delle obbligazioni connesse al contratto che è alla base di quell'operazione[103]. Si tratta di un sistema che, al di là delle regole nazionali e internazionali di diritto privato,

[101] Fonte: Croman K. *et al*., "On Scaling Decentralized Blockchains", 2016.
[102] Fonte: Michele Faioli *et al*., 2019.
[103] Fonte: Michele Faioli, "*Con la Blockchain migliorano politiche del lavoro e previdenza*", SOLE24ORE, 2018.

garantisce la veridicità e l'immodificabilità di un dato informatico senza che vi sia il contributo o il controllo di un ente centrale (questo avviene invece per le operazioni in valuta FIAT, dove la veridicità e l'immodificabilità sono garantiti dai processi di certificazione delle banche). Ogni tipo di operazione e di rapporto fra due o più soggetti giuridici potrà divenire, vero, certo e immodificabile grazie alla Blockchain. Per questo è fondamentale sottolineare le potenzialità di questa tecnologia, perché i suoi sviluppi andranno potenzialmente al di là della nostro attuale orizzonte giuridico. Si comprende allora l'importanza di figure professionali che siano in grado di trasmutare contenuti giuridici complessi in un linguaggio che sia comprensibile per i programmatori che creeranno la struttura comunicativa della Blockchain.

Il lavoro del giurista, come sappiamo, è stato quello di saper prevedere quali effetti possono realizzarsi al verificarsi o meno di determinate condizioni. Ciò che cambierà non è dunque il fine, ma gli strumenti: questo fenomeno tecnologico impone una certa evoluzione delle strutture logiche del pensiero giuridico, che dovrà sforzarsi per diventare facilmente comprensibile per la macchina informatica[104]. Le clausole contrattuali degli *smart contract* devono infatti essere

[104] Fonte: KIVIAT T. L., "Beyond bitcoin: Issues in regulating blockchain transactions", Duke Law Journal, 65, pp. 569-698, 2014.

pensate e costruite per essere operate dai computer, pur producendo effetti concreti e non soltanto virtuali[105].

Le prime idee circa la possibilità di creare dei contratti che fossero *self-executing*[106] e *self-enforcing*[107] erano state immaginate già prima dell'avvento della Blockchain. Ciò che mancava era riuscire a potenziare quest'idea per portarla sul piano operativo: operazione che potrà essere realizzata grazie alla caratteristica di decentralizzazione che presentano gli *smart contract* basati sulla Blockchain[108]. Poiché decentralizzati, infatti, non necessitano di un'istituzione terza che ne curi l'operatività, ne validi i contenuti e che ne produca l'effettività connessa agli eventi giuridici[109]. "*La Blockchain è per sua natura liberamente programmabile, potendo al contempo essere strutturata per essere self-enforcing, cioè auto-esecutiva*"[110]: risulta quindi possibile, con e tramite la Blockchain, superare un sistema civilistico basato sull'autorità terza che certifica, verifica e coattivamente mette in esecuzione le clausole contrattuali.

Quello dello *smart contract* è un modello che, come già detto, è ancora in larga parte da definire: l'obiettivo comune di informatici e giuristi all'opera su questa

---

[105] Fonte: "*Blockchain e smart contract: questioni giuridiche aperte*", Lorenzo Parola, Paola Merati, Giacomo Pavotti, 2018.
[106] Letteralmente "autoesecutivi".
[107] (diritto, economia) che si autosostiene; (riferito a norme, contratti) che è interesse di ciascuno rispettare.
[108] Fonte: Michele Faioli, Emanuele Petrilli, Donato Faioli, "*Blockchain, contratti e lavoro. La ri-rivoluzione digitale nel mondo produttivo e nelle PA*", 2019.
[109] Fonte: Nick Szabo, "*Formalizing and Securing Relationships on Public Networks*", 1997.
[110] Fonte: Michele Faioli, Emanuele Petrilli, Donato Faioli, "*Blockchain, contratti e lavoro. La ri-rivoluzione digitale nel mondo produttivo e nelle PA*", 2019.

stimolante fattispecie consiste nell'individuazione di uno strumento, utilizzabile nella vita quotidiana, che risponda sia alle esigenze di completezza dell'ordinamento giuridico che a quelle matematiche del sistema binario[111]. In sintesi, lo scopo della ricerca comune è quello di verificare se il giudizio ipotetico-prescrittivo (se c'è A ci deve essere B) tipico delle norme giuridiche possa essere applicato a un target di analisi molto particolare[112]: la scrittura di un codice informatico che renda *self-executing* alcune clausole contrattuali, risolvendo in radice dei problemi collegati a loro inadempimento.

3.1.1 Nascita e diffusione degli smart contract

L'idea di *smart contract* ha preso forma per la prima volta nel 1997 nei due paper a firma di Nick Szabo "*Formalizing and Securing Relationships on Public Networks*" e "*The Idea of Smart Contracts*", in cui l'autore prendeva spunto dal sistema di vendita dei distributori automatici per teorizzare il trasferimento di alcuni diritti in esecuzione di un algoritmo, definendo, appunto, lo *smart contract* come "*un protocollo di transazione computerizzato che esegue i termini di un contratto*"[113].

[111] Fonte: Faioli *et al*., 2019.
[112] Fonte: Ethereum White Paper, "*A next generation smart contract & decentralized application platform*", Vitalik Buterin, 2014.
[113] Fonte: Nick Szabo, 1997: "*The Smart contract is a computerized transaction protocol that executes the terms of a contract*".

Nel 1998 Nick Szabo formalizzava in un terzo paper intitolato "*Secure Property Titles with Owner Authority*" i concetti già individuati nei due precedenti lavori. Nello stesso anno Wei Dai esponeva nell'opera "*B-money*" (*cap. 1, par. 1.1*) l'idea di un protocollo contrattuale indipendente da attuare in un network non tracciabile fra soggetti identificati da uno pseudonimo digitale (la chiave crittografica pubblica): il sistema prevedeva lo scambio di messaggi firmati digitalmente e crittografati e la predeterminazione delle regole di *enforcement*[114].

Pur nelle differenze logiche fra le opere citate, gli schemi teorizzati dai due autori appaiono idonei ad esiti *self-enforcing* di quelle clausole che, essendo giuridicamente eseguibili, consentano altresì un'idonea determinazione computazionale.

Nello specifico, la proposta formulata da Szabo nel paper "*Secure Property Titles with Owner Authority*" consiste in una *securitization*[115] digitale all'interno di una rete *pee-to-peer* (*cap. 1, par. 1.3.1*): uno specifico diritto di proprietà viene incorporato in un titolo destinato alla circolazione, assieme alle informazioni ad esso relative; il suo trasferimento è messo in sicurezza crittografica e il titolo è

[114] Fonte: Wei Dai, "*B-Money*", 1998: "*The enforcement of contracts. If the parties to a contract cannot agree on an appropriate conclusion even with the help of the arbitrator, each party broadcasts a suggested reparation/fine schedule and any arguments or evidence in his favor. Each participant makes a determination as to the actual reparations and/or fines, and modifies his accounts accordingly*".

[115] Operazione mediante la quale un insieme di diritti su attività illiquide (crediti, immobili) sono incorporati in uno strumento negoziabile. In altre parole, la *securitization*, o cartolarizzazione, è una tecnica finanziaria progettata per trasformare strumenti finanziari non trasferibili in altri strumenti finanziari trasferibili, quindi negoziabili. Fonte: www.borsaitaliana.it.

inserito in una catena logica di titoli analoghi a garanzia della continuità delle operazioni. L'intero database contenente tutti i titoli codificati è reso pubblico, cioè replicato su tutti i computer della rete in maniera da assicurare che la custodia e il trasferimento dei titoli avvengano correttamente[116].

A distanza di più di vent'anni il sistema ideato da Nick Szabo appare ancora attuale e contiene in sé una serie di input utili per lo sviluppo del sistema di contrattazione *smart*.

3.1.2 Struttura e modalità di funzionamento

Gli *smart contract*, come li conosciamo oggi, rappresentano la traduzione o trasposizione in codice di un contratto al fine di verificare in automatico l'avverarsi di determinate condizioni (controllo dei dati di base del contratto) e di auto-eseguire azioni (o dare disposizione affinché si possano eseguire determinate azioni) nel momento in cui le condizioni determinate tra le parti sono raggiunte e verificate[117]: si costituiscono, pertanto, di un codice che "legge" sia le clausole che sono state concordate sia le condizioni operative nelle quali esse devono verificarsi, e si auto-eseguono nel momento in cui le condizioni reali corrispondono a quelle concordate.

---

[116] Fonte: "*Distributed ledger technologies e sistemi di Blockchain: digital currency, smart contract e altre applicazioni*", Maria Letizia Perugini, 2018.
[117] Fonte: www.blockchain4innovation.it.

È evidente, pertanto, che lo *smart contract* ha bisogno di un supporto legale per la sua stesura, ma non per la sua verifica e attivazione. E proprio perché l'assenza di un intervento umano corrisponde anche all'assenza di un contributo interpretativo, lo *smart contract* deve essere basato su descrizioni estremamente precise che devono compendiare tutte le circostanze, le condizioni e le situazioni possibili[118]. Pertanto, la gestione dei dati, e dei *big data* in particolare, diventa un fattore critico essenziale per stabilire la qualità dello *smart contract*. Infatti, è fondamentale circoscrivere in modo estremamente preciso le fonti di dati alle quali il contratto è chiamato ad attenersi. Tali dati vengono poi elaborati in modo deterministico, cioè producendo identici risultati a fronte di identiche condizioni iniziali: in altre parole, se gli input sono gli stessi i risultati saranno sempre i medesimi. La logica di funzionamento, pertanto, è quella "*if this then that*": se si verifica un presupposto (*this*) allora consegue un risultato (*that*)[119].

Da un lato il meccanismo di attivazione dei contratti *smart* rappresenta una sicurezza in quanto garantisce alle parti un giudizio assolutamente oggettivo, escludendo qualsiasi forma di interpretazione e discrezione, dall'altro sposta sul codice e sulla programmazione il peso, la responsabilità e il potere di decidere.

Fino ad ora non è stato esplicitato se e perché uno *smart contract* per funzionare abbia bisogno necessariamente di una struttura Blockchain. Infatti, le sue

[118] Fonte: www.blockchain4innovation.it.
[119] Fonte: "*Blockchain e smart contract: funzionamento e applicazioni*", Francesca Arrigo, 2019.

caratteristiche intrinseche gli consentono di affidarsi semplicemente a strumenti digitali, nello specifico ad un codice di scrittura e ad una piattaforma generica. Tuttavia, uno *smart contract* deve primariamente garantire che il codice con cui è stato scritto non possa essere modificato, che le fonti di dati che determinano le condizioni di applicazione siano certificate e affidabili e che le modalità di lettura e controllo di tali fonti siano a loro volta certificate e deterministiche[120]. E il network Blockchain, con le sue caratteristiche di decentralizzazione ed immutabilità, assicura l'esecuzione del contratto trasposto nel codice software[121].

È necessario, a questo punto, procedere con una breve spiegazione di come la tecnologia Blockchain si applichi ad uno *smart contract* e di come un contratto possa materialmente assumere una forma tecnologica, diversa dal linguaggio naturale. Le informazioni di seguito riportate saranno anche illustrate schematicamente in *figura 21*.

Uno *smart contract* è costituito da tre elementi principali: un account, ossia la combinazione delle chiavi private dei due contraenti e la chiave pubblica posseduta dal resto del network Blockchain per verificare le informazioni, una quota della memoria del registro distribuito che esso occupa e un codice di esecuzione. Solo al momento della stesura del contratto si renderà necessario l'intervento delle due parti, che dovranno deciderne di comune accordo i termini,

[120] Fonte: "*Smart Contracts: che cosa sono, come funzionano quali sono gli ambiti applicativi*", Mauro Bellini, 2018.
[121] Fonte: "*Come scrivere uno smart contract*", Claudia Morelli, 2019.

ossia le clausole che ne faranno parte. Ogni clausola viene pertanto discussa e, una volta approvata da entrambi i contraenti, inserita tramite le chiavi crittografate private in un blocco, e da linguaggio naturale viene poi trasformata in linguaggio crittografico in grado di essere compreso dal sistema[122]. Il blocco verrà quindi vagliato dagli altri nodi, i cosiddetti *miner*, che, tramite la chiave pubblica, potranno effettivamente verificare la validità delle informazioni contenute nel blocco. Una volta approvato, quest'ultimo verrà aggiunto al resto dei blocchi e contribuirà a formare la catena. Infine, grazie alla sequenza "*if-then*", se il sistema registrerà l'avveramento del fatto di cui alla clausola, il contratto progredirà; se, al contrario, il contenuto della clausola verrà violato, il contratto attiverà automaticamente i rimedi previsti dalle parti stesse o dalla legge[123].

[122] Fonte: "*Blockchain e smart contract: funzionamento e applicazioni*", Francesca Arrigo, 2019.
[123] Fonte: "*Elementi accessori del contratto: la condizione*", Francesco Pittaluga, 2005.

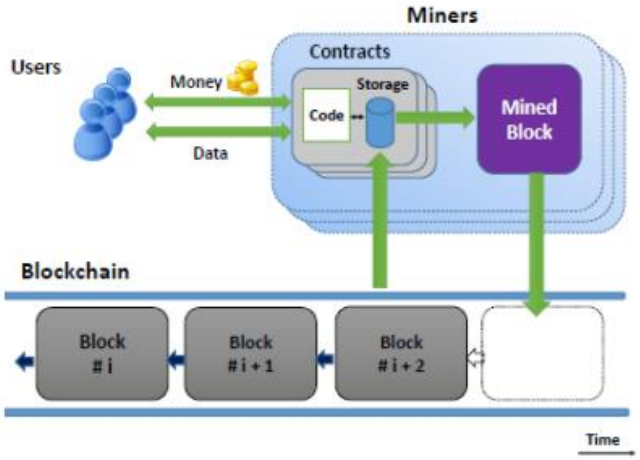

Figura 21. Il flusso seguito dalle varie clausole di un contratto per essere codificate in linguaggio macchina e inserite nella Blockchain. Fonte: Maher Alharby, Aad Van Moorsel, "Blockchain-based smart contracts: A systematic mapping study", 2017.

Gli *smart contract* possono essere sviluppati e implementati tramite diverse piattaforme Blockchain, ciascuna delle quali può offrire funzioni e caratteristiche differenti e supportare linguaggi di programmazione più o meno complessi[124]. Di seguito si elencano le principali piattaforme utilizzate per la stesura di un contratto intelligente.

La piattaforma **Bitcoin** offre la possibilità di creare *smart contract*, pur avendo una capacità computazionale molto limitata e un linguaggio di programmazione ristretto: il sistema permette di realizzare contratti con una logica semplice per processare singole transazioni. **NXT**, Blockchain pubblica come Bitcoin, permette

[124] Fonte: "*Blockchain-based smart contracts: a systematic mapping study*", Maher Alharby, Aad van Moorsel, 2017.

ai suoi clienti di creare *smart contract* utilizzando solamente dei modelli prestabiliti, senza la possibilità di *customizzarli* ulteriormente. Tramite **Ethereum**, la più famosa piattaforma per la programmazione dei contratti *smart*, invece, questi ultimi sono codificabili utilizzando il linguaggio *Solidity*, la cui sintassi è fortemente influenzata da *JavaScript*, consentendo istruzioni di codice anche complesse, ramificate e in loop. La piattaforma rende quindi possibile la creazione di strutture di qualsiasi tipo, personalizzabili in vari modi, includendo ramificazioni logiche più complesse come loop, limiti revocabili, etc. Un'altra piattaforma, **NEM**, è ancora più scalabile di Ethereum: a fronte di 15 transazioni al secondo di quest'ultima ne può gestire centinaia. È inoltre più sicura e fornisce un codice di programmazione più leggero. **EOS**, inoltre, che grazie alla community Crypto sta diventando sempre più popolare dato il costo irrisorio e la velocità di transazione per secondo, consente di programmare utilizzando il linguaggio *C++*, aumentando la flessibilità di creazione degli *smart contract*. È opportuno inoltre citare **Aion**, piattaforma di contrattazione intelligente che consente l'interscambio di transazioni e messaggi tra diverse Blockchain tramite i suoi innovativi protocolli. I linguaggi utilizzabili sono *Python* o *Groovy*. Proseguendo con l'elenco troviamo i contratti intelligenti di **Hyperledger Fabric** (HLF), noti come *chaincode*. HLF è scritto in lingua *Go*, il linguaggio di programmazione open source di Google. **Corda**, infine, è una piattaforma di

contratto intelligente nata recentemente, ideale per la creazione di accordi finanziari, che utilizza linguaggi di programmazione *JVM* come *Java* o *Kotlin*.

3.1.3 Blockchain e smart contract: limiti d'impiego

Nonostante gli innumerevoli vantaggi connessi agli *smart contract*, le criticità legate al loro utilizzo sono ancora molte.

Secondo alcune ricerche[125] il tasso medio di fallimento di uno *smart contract* all'interno della Blockchain Ethereum (piattaforma specializzata per l'elaborazione dei contratti *smart*) si aggira attorno al 3%. Tuttavia, se si pensa alla famosa vicenda The DAO[126] del 2016, in cui un gruppo di hacker è riuscito nella sottrazione di una ingente somma di denaro appartenente al fondo di Ethereum approfittando di un bug all'interno dello *smart contract* (nello specifico, riproducendo una condizione non prevista dalla struttura del contratto), il difetto

[125] Lee, 2018.

[126] L'acronimo DAO sta per *Decentralized Autonomous Organization* (in italiano, Organizzazione Autonoma Decentralizzata). In poche parole, una DAO è un'organizzazione governata da codice e programmi informatici. Come tale, ha la capacità di funzionare in modo autonomo, senza bisogno di un'autorità centrale. Uno dei primi esempi di DAO è stato "The DAO" che, in qualità di organizzazione virtuale, è stata creata all'interno della Blockchain Ethereum con lo scopo di raccogliere fondi da investitori per finanziare progetti e startup che lavorano in ambito *smart contracts*. Tuttavia, poco dopo il lancio, circa un terzo dei fondi è stato rubato in uno dei più grandi hack nella storia delle criptovalute. Il DAO attacker, nel giugno 2016, è riuscito infatti a spostare fuori dalla DAO oltre 3.6 milioni di Ether, corrispondenti a circa 60 milioni di dollari (considerando il tasso di cambio precedente all'attacco). Fonte: www.academy.binance.com.

all'interno della struttura ha portato ad una colossale perdita quantificabile in circa 3,6 milioni di Ether[127].

Molte sono le classificazioni e le analisi volte ad identificare i punti di debolezza della relazione tra *smart contract* e Blockchain, ma in questo paragrafo si vuole evidenziare la *clusterizzazione* proposta dalla ricerca condotta da Maher Alharby e Aad van Moorsel nel 2017[128], che hanno provveduto all'analisi e alla sintesi di diversi paper riguardanti l'argomento.

Di seguito sono esplicate le quattro categorie principali evidenziate dallo studio[129]:

1. *Codifying issues*: si tratta dei principali ostacoli allo sviluppo di un contratto (inerentemente alla difficoltà nella scrittura di un contratto corretto, all'incapacità di modificare lo stesso o terminarlo, alla complessità dei linguaggi di programmazione);
2. *Security issues*: fanno riferimento ad eventuali bug o vulnerabilità del sistema di contrattazione intelligente tramite cui enti malintenzionati possono lanciare un attacco (solitamente, attraverso l'alterazione del *time-stamp*);

[127] Fonte: "*The DAO e possibili fork di Ethereum*", Federico Tenga, 2016.
[128] Maher Aharby e Aad Van Moorsel, "*Blockchain-based smart contracts: a systematic mapping study*", 2017.
[129] Fonte: Maher Alharby e Aad Van Moorsel, "*Blockchain-based smart contracts: a systematic mapping study*", 2017.

3. *Privacy issues*: riferiti alla pubblicazione delle caratteristiche del contratto a persone non direttamente coinvolte (mancanza di privacy nella transazione);
4. *Performance issues*: che possono limitare l'abilità della struttura Blockchain di diventare scalabile (in genere, tramite l'esecuzione sequenziale degli *smart contract*).

Analizzando il primo punto, concernente i limiti della codifica del contratto, si identificano diverse sfide che possono presentarsi agli sviluppatori. Prima fra tutte, la difficoltà di stipulare contratti che siano corretti, nel senso che effettivamente funzionino nel modo in cui è stato deciso dalle due parti. Una soluzione a questo problema, evidenziata dalla letteratura, può essere identificata nell'utilizzo di sistemi per la creazione di contratti semi-automatici[130], ossia in grado di leggere il contratto scritto in linguaggio naturale dalle due parti e tradurlo in opportune regole. Parallelamente a ciò, è possibile utilizzare anche sistemi di verifica in grado di indagare circa l'eventuale presenza di situazioni indesiderate erroneamente incluse nel contratto. Data inoltre l'immutabilità della Blockchain, è intuibile che uno *smart contract* non possa essere modificato una volta eseguito: a tal proposito, sono stati identificati in letteratura degli standard che permettono di scrivere regole in grado di essere modificate o terminate. La complessità di alcuni

[130] Fonte: Maher Alharby e Aad Van Moorsel, "*Blockchain-based smart contracts: a systematic mapping study*", 2017.

linguaggi di programmazione, in aggiunta, può rendere ancor più difficoltosa la stesura di un contratto intelligente. Tramite linguaggi come *Solidity*, ossia di tipo procedurale, il codice è eseguito come una successione di step in cui il programmatore deve specificare cosa deve essere fatto prima e cosa dopo, rendendo la scrittura dell'accordo molto laboriosa. Ecco che l'utilizzo di linguaggi di tipo logico permette, da un lato, di non dover specificare al sistema la sequenza dei passi da eseguire, rendendo tuttavia, dall'altro, molto costosi gli algoritmi di programmazione.

Relativamente alle *security issues*, sottolineano gli Autori, la dipendenza dal *time-stamp*, ossia la marcatura dei blocchi che rende possibile avviare ed eseguire le transazioni, può dare adito a ulteriori vulnerabilità del contratto. Generalmente infatti il *time-stamp* di un blocco viene settato come l'orario locale del *miner* che ha generato il blocco. Tuttavia, se un nodo disonesto riesce ad alterare questa data fino a un massimo di circa 15 minuti rispetto a quella corretta, il blocco viene comunque considerato valido, generando una debolezza intrinseca in tutti quei contratti che si basano sull'accuratezza della marca temporale. Se inoltre due transazioni dipendenti tra di loro che invocano lo stesso contratto sono contenute all'interno di uno stesso blocco si può incorrere in un altro tipo di problema, noto come interdipendenza tra le transazioni. Il suggerimento per risolvere questo problema arriva da una funzione intrinseca alla struttura Ethereum, ossia la

funzione *SendIfReceived*[131], che autorizza una transazione solamente quando un'altra che fa riferimento allo stesso contratto viene prima accettata da tutti i nodi e, naturalmente, eseguita.

Per quanto riguarda le *privacy issues*, che fanno riferimento al problema della mancanza di privacy dei contratti, è intuibile che la crittazione di un contratto prima di inviarlo tramite Blockchain permetterebbe di renderlo visibile solamente a chi, come i partecipanti o chi è coinvolto nel contratto, ne possiede le chiavi di decodifica (*cap. 2, par. 2.1.2*).

Infine, in relazione all'ultima classe di problematiche connesse al tema della contrattazione *smart*, migliori performance possono essere raggiunte sostituendo la tradizionale esecuzione sequenziale di contratti (esecuzione di un contratto per volta) con l'elaborazione in parallelo di contratti purché siano tra di loro indipendenti.

In via conclusiva, dalle analisi finora presentate, si evince facilmente che uno *smart contract* è una tecnologia relativamente spinosa, poiché il compito principale a cui è chiamata oggi è quello di rendere eseguibile in maniera deterministica la complessità di un contratto personalizzato e stabilito da due parti, catalogando tutte le possibili condizioni e situazioni verificabili in linguaggio macchina. Gli *smart contract* sono oggi ancora molto vulnerabili e,

[131] Fonte: Maher Alharby e Aad Van Moorsel, "*Blockchain-based smart contracts: a systematic mapping study*", 2017.

soprattutto, dipendenti da condizioni e fattori esterni all'ambiente in cui sono stati sviluppati, quindi di difficile previsione.

Esistono in commercio diversi progetti volti allo sviluppo e al supporto dei contratti *smart*. Per citarne uno, il programma Quantstamp permette di esaminare nel dettaglio la struttura dell'accordo e di individuare eventuali bug di sistema (anche se il processo di verifica è piuttosto dispendioso in termini di tempo e risorse), ma di identificare solamente gli errori già presenti, senza certificare la loro effettiva assenza. Tale limite è superato da un altro programma, CertiK, che tramite algoritmi matematici modulari testa la resistenza della piattaforma ad eventuali attacchi di malintenzionati.

L'incorruttibilità dei contratti intelligenti, caratteristica fondamentale propria della struttura Blockchain su cui poggiano, li rende senz'altro attraenti e profittevoli per molti ambiti. Tuttavia, questa peculiarità ha un punto debole: la rigidità. Impossibile predire ogni conseguenza di un accordo a priori. Impossibile inoltre esser in grado di realizzare contratti sufficientemente complessi e totalmente privi di errori: scenari inaspettati, infatti, sono sempre in agguato. Fino a che non si troverà una soluzione alla necessaria flessibilità di questi contratti, errori da un lato e cause di forza maggiore dall'altro minacceranno l'affidabilità del patto tra le parti, rendendolo vulnerabile. Fortunatamente diversi gruppi di ricerca in varie parti del mondo stanno lavorando per migliorare questo limite. Nel frattempo, è

bene che chiunque si voglia approcciare all'uso o alla conoscenza degli *smart contract* sia in grado di capirne tutti i potenziali rischi così come i benefici.

3.2 Token e ICO

Il *token* e l'ICO sono due ingegnosi strumenti, creati all'interno del mondo Blockchain, in grado di realizzare nuovi modelli di business ma che ad oggi sono privi del necessario supporto normativo che garantisca agli utilizzatori certezza del diritto acquisito mediante l'acquisto di detti strumenti.

Nello specifico, un *token* è un'informazione digitale, registrata su un registro distribuito, quale appunto la Blockchain, univocamente associata a uno e un solo specifico utente del sistema e rappresentativa di una qualche forma di diritto: la proprietà di un asset, l'accesso ad un servizio, la ricezione di un pagamento, e così via[132]. Le caratteristiche dei registri distribuiti permettono di creare *token* unici, definire i diritti a essi associati, trasferirne la proprietà a un valore stabilito da regole di mercato ed eventualmente anche distruggerli. Inoltre, grazie agli algoritmi con i quali operano le *distributed ledger tecnologies*, viene garantita l'impossibilità di effettuare una "double-spending" dei propri *token* (*cap. 2, par. 2.1.5*), anche in assenza di un'autorità centrale. È opportuno sottolineare che ogni

[132] Fonte: Blockchain & Distributed Ledger, "*Initial Coin Offer (ICO) e Token*", Valeria Portale, 2019.

bene, prodotto e servizio può essere trasformato in *token* (fenomeno denominato "*tokenizzazione*"). E la Blockchain è lo strumento che permette gli scambi di *token* in maniera sicura e senza intermediari. Essendo inoltre programmabile, permette di utilizzare gli *smart contract* per creare nuovi *token*. In altre parole, creare un *token* sulla Blockchain vuol dire definire in uno *smart contract* tutte le sue caratteristiche fondamentali, come ad esempio il numero di *token* in circolazione, chi è abilitato a trasferirli, coloro che possono disporre dei *token* (i cosiddetti "*token* holder"), le regole di accesso ai *token*, e così via.

Esistono diverse tipologie di *token* determinate sia dal tipo di approccio tecnologico sia dal tipo di utilizzo. In particolare è importante focalizzare l'attenzione su tre diverse tipologie di *token* determinate dal tipo di diritti gestiti dagli stessi[133]:

1. ***Token* di classe 1**: il *token* si presenta come una vera e propria moneta (*coin*) che può essere trasferita tramite transazioni su Blockchain. Si tratta di una tipologia di *token* che non conferisce al proprietario diritti nei confronti di una controparte, ma ha la funzione di registrare un diritto di proprietà del *token* stesso o l'esistenza di un determinato soggetto/oggetto. Possedendo questo tipo di *token* il proprietario non ha diritti ulteriori rispetto a quelli correlati alla proprietà del *token* stesso. Fanno parte della classe 1 i *token* di criptovalute come Bitcoin, Bitcoin Cash, Litecoin, etc.;

[133] Fonte: Valeria Portale, 2019.

2. ***Token* di classe 2**: questa casistica include i *token* che sono in grado di conferire ai proprietari diritti che possono essere esercitati nei confronti del soggetto che ha generato i *token* (o eventualmente nei confronti di terzi). In altre parole, i *token* di classe 2 potrebbero essere definiti come una sorta di titoli di credito, ossia di "documenti" che conferiscono al possessore "*diritto alla prestazione in esso indicata verso presentazione del titolo*"[134]. Più nello specifico, si tratta di:
    - ***token* per *smart contract* relativi alla gestione di pagamenti futuri**, che garantiscono cioè il conferimento di un diritto a ricevere dei pagamenti futuri, sulla base di determinate condizioni stabilite a livello contrattuale che il *token* è chiamato a gestire in modo "automatico";
    - ***token* come asset**, intesi cioè come una sorta di diritto di proprietà di un determinato asset, sia materiale che immateriale (rappresentando, ad esempio, una quota di partecipazione dell'entità giuridica emittente o di entità terze);
    - ***token* per pagamenti standardizzati**, utilizzati solitamente quando una persona vanta il diritto di ricevere un pagamento per un importo specifico ben definito;

[134] Fonte: Art. 1992 c.c.

- ***token* per la gestione di prestazione di servizi**. In questa circostanza il titolare del *token* vanta il diritto di ricevere una determinata prestazione dal soggetto emittente o da un terzo che abbia sottoscritto un accordo commerciale.

3. ***Token* di classe 3**: questa fattispecie, infine, delinea *token* che sono in grado di conferire al proprietario diversi diritti, come ad esempio il diritto di voto, o diritti di tipo economico per i rappresentanti legali o soci di una società, etc.

Oltre alle circostanze finora enunciate, i *token* possono essere venduti dall'avente titolo, attraverso specifici contratti in ambito Blockchain, per finanziare altre iniziative. Di fatti, la possibilità di "*tokenizzare*" asset, prodotti e servizi ha aperto la possibilità di utilizzare la vendita di *token* come forma di finanziamento di nuove iniziative progettuali basate su Blockchain e DLT[135]. Ed è qui che entra in gioco l'idea di ICO, acronimo di *Initial Coin Offering*.

Le ICO, propriamente, rappresentano l'azione di generare e vendere agli investitori interessati un nuovo *token*, con l'obiettivo di finanziare lo sviluppo di un particolare progetto[136]. Potremmo definirle come uno sforzo di crowdfunding[137] pubblico, il cui scopo è quello di aiutare una nuova idea o

[135] Fonte: "*ICO Initial Coin Offering: una ricostruzione giuridica del fenomeno*", Massimiliano Nicotra, 2019.
[136] Fonte: Valeria Portale, 2019.
[137] Il crowdfounding, o finanziamento collettivo, è un processo collaborativo di un gruppo di persone che utilizza il proprio denaro in comune per sostenere gli sforzi di persone e

progetto a prendere forma. Lo sviluppo del progetto, infatti, avverrà con l'aiuto dei finanziamenti reperiti mediante la vendita di detti *token* da parte dell'ente emittente, che gli investitori decideranno di acquistare credendo nel buon fine del progetto stesso[138]. Il *token* relativo ad un ICO può essere associato anche a diritti diversi rispetto a quelli garantiti dalle azioni e dalle obbligazioni, come ad esempio l'accesso al servizio sviluppato dal progetto.

Nello specifico, Il termine *Initial Coin Offering* deriva dal più tradizionale *Initial Public Offering* (IPO) utilizzato per indicare l'offerta pubblica di titoli di una società che intende quotarsi per la prima volta sul mercato azionario[139]. Le due procedure hanno entrambe l'obiettivo di raccogliere capitali per la realizzazione di un progetto; una ICO differisce tuttavia in due aspetti fondamentali[140]:

1. nell'oggetto principale dell'offerta, che nel caso specifico è un *coin* o *token*;
2. nel luogo in cui questa offerta si svolge, che non è un mercato regolamentato, ma una piattaforma Blockchain.

---

organizzazioni. Il termine indica propriamente il processo con cui più persone ("folla" o crowd) conferiscono somme di denaro (funding), anche di modesta entità, per finanziare un progetto imprenditoriale o iniziative di diverso genere utilizzando siti internet ("piattaforme" o "portali") e ricevendo talvolta in cambio una ricompensa. Fonte: www.consob.it.

[138] Fonte: "*ICO Initial Coin Offering: una ricostruzione giuridica del fenomeno*", Massimiliano Nicotra, 2019.

[139] Fonte: www.blog.osservatori.net.

[140] Fonte: Massimiliano Nicotra, 2019.

Nello specifico, il processo di realizzazione di una ICO può essere descritto in quattro fasi principali[141]:

1. Stesura di un **whitepaper** che descriva il progetto e il suo stato di avanzamento, il fabbisogno di finanziamento, quanti *token* resteranno in mano ai fondatori, con quali (cripto)valute si potranno acquistare i *token* e quanto durerà la campagna;
2. Attività di **comunicazione** che spesso si svolge creando pagine di discussione ad hoc per promuovere l'ICO e attrarre potenziali investitori;
3. Acquisto dei ***token*** da parte degli investitori. Se non vengono raggiunti gli obiettivi di raccolta, i fondi vengono restituiti agli investitori. Se invece vengono raggiunti i requisiti, i fondi raccolti vengono utilizzati per iniziare o completare il progetto;
4. Al termine della vendita iniziale, i *token* vengono inseriti nei listini degli **Exchange** e possono essere scambiati tra gli utenti.

In merito al fenomeno delle ICO, è possibile approfondire la vicenda "The DAO", accennata nel *paragrafo 3.1.2* del presente capitolo. Infatti, uno dei provvedimenti più rilevanti sulle *Initial Coin Offering* è quello del 25 luglio 2017 da parte della U.S. Security and Exchange Commission relativo al Report di investigazione su

[141] Fonte: Pezzuto Antonio, "*Brevi note sulle Initial Coin Offerings (ICOs)*", Studio Legale Tidona e Associati, Rivista di diritto Bancario e Finanziario, 2019.

The DAO[142]. La vicenda, come accennato, è stata uno dei primi eventi di ampia rilevanza relativo alla tecnologia Blockchain ed ha coinvolto numerosi soggetti, dando origine al fork (ossia alla "spaccatura") della Blockchain Ethereum. Riprendendone la definizione, The DAO è intesa come "*Decentralized autonomous organization*", un'organizzazione creata sulla Blockchain di Ethereum (tramite una serie di *smart contract* correlati) caratterizzata dal fatto di non essere formalmente definita: cioè un'organizzazione senza una sede, senza una personalità giuridica, senza veri e propri amministratori. I creatori di The DAO, per costituire tale organizzazione, hanno seguito i vari passaggi che vengono usualmente effettuati per la realizzazione di una ICO: creazione di un sito Internet per fornire informazioni, redazione di un whitepaper in cui viene descritto il progetto, audit del codice sorgente degli *smart contracts* utilizzati, accordi con alcuni Exchange per permettere lo scambio dei *token* una volta acquisiti, etc[143]. L'obiettivo di The DAO era quello di raccogliere capitali (tramite lo scambio di *DAO Tokens* a fronte di ETH) da investire su progetti che venivano previamente vagliati da un comitato e successivamente posti in votazione ai possessori di *DAO Tokens*. Questi ultimi potevano esprimere il loro voto (proporzionale al quantitativo di *token* posseduti) per determinare in favore di quali progetti sarebbero stati erogati i capitali. Nel giro di pochi mesi gli

[142] Fonte: Massimiliano Nicotra, 2019.
[143] Fonte: Studio Legale Tidona e Associati, Rivista di diritto Bancario e Finanziario, Antonio Pezzuto, "*Brevi note sulle Initial Coin Offerings (ICOs)*", 2019.

organizzatori di The DAO riuscirono a raccogliere circa 150 milioni di dollari. Tuttavia, Il 18 giugno 2016 veniva violato l'indirizzo in cui erano allocati gli ETH ricevuti dall'organizzazione ed in poche ore furono persi circa 60 milioni di dollari. La SEC[144], nell'analizzare la vicenda, si è posta l'obiettivo di qualificare la fattispecie, soprattutto per comprendere la riconducibilità o meno della stessa nell'ambito dell'attività di collocamento di strumenti finanziari e, conseguentemente, poter quindi stabilire se il caso di specie fosse regolato o meno dalla "*Securities Law*" statunitense. Il test effettuato dalla SEC prevedeva che per comprendere se la fattispecie concreta potesse esser definita un "contratto di investimento" era necessario riferirsi alla sostanza e non alla mera forma contrattuale, considerando come contratto di investimento qualsiasi investimento di denaro in un'impresa con la ragionevole aspettativa di profitti derivanti da sforzi manageriali o imprenditoriali di altri[145]. Nel caso di The DAO la SEC ha evidenziato che:

- gli investitori avevano scambiato Ether (che avevano un valore determinato sul mercato) in cambio di *DAO Tokens*;
- l'investimento era stato effettuato con un'aspettativa di profitto. Tutti i materiali promozionali di The DAO, infatti, evidenziavano che l'obiettivo

[144] Acronimo di "Security and Exchange Commission".
[145] Fonte: "*Il regime giuridico delle ICOs. Analisi comparata e prospettive regolatorie italiane*", Avv. Massimiliano Nicotra, 2019.

era quello di creare un'entità con scopo di lucro, la quale avrebbe dovuto finanziare progetti in cambio di un ritorno sull'investimento;

- l'aspettativa di ritorno dell'investimento dipendeva da sforzi gestionali altrui, dato che l'organizzazione di The DAO sulle decisioni in merito ai progetti da finanziare era assolutamente verticistica. I fondatori dell'organizzazione ed i curatori monitoravano costantemente le attività, salvaguardavano gli interessi degli investitori e decidevano quali progetti dovevano essere sottoposti al voto.

Tali considerazioni hanno indotto la SEC a ritenere i *DAO Tokens* strumenti finanziari, con conseguente applicazione della "Securities Law", dalla quale deriva l'obbligo per l'ente emittente di registrare le offerte e vendite degli strumenti (obbligo non rispettato dagli organizzatori di The DAO) e, correlativamente, l'obbligo di registrazione per i soggetti che offrivano piattaforme di scambio (trading) dei suddetti *token*.

È possibile affermare, dunque, che, pur non costituendo una vera e propria regolamentazione del fenomeno, il Report SEC del 25 luglio 2017 ha svolto la funzione di spartiacque. Nel periodo immediatamente successivo alla sua emissione si sono infatti susseguite varie prese di posizione da parte delle autorità di controllo di numerosi Paesi del mondo[146].

[146] Fonte: "*Il regime giuridico delle ICOs. Analisi comparata e prospettive regolatorie italiane*", Avv. Massimiliano Nicotra, 2019.

3.3 Blockchain in ambito aziendale

Negli ultimi anni varie società di consulenza hanno pubblicato oltre 500.000 report sui possibili impatti a livello aziendale della Blockchain, che approfondiscono le possibilità offerte da tale tecnologia per migliorare l'efficienza, la qualità e la rapidità decisionale ed esecutiva; ossia, per fare le stesse cose, ma meglio[147]. In questa sezione approfondiremo, nello specifico, il possibile impatto della Blockchain sui modelli e le strategie di business delle aziende, sulla loro missione e visione, nonché sulla governance aziendale e sociale, ossia sul "territorio" nel quale le aziende stesse si trovano a operare. L'ambizione è dunque riflettere su come tale tecnologia possa permettere di fare cose diverse, o le stesse cose in modo diverso[148].

Secondo una survey condotta dal World Economic Forum, entro il 2027 il 10% del PIL globale sarà sviluppato su piattaforme Blockchain. Tale tecnologia non si limiterà a permettere transazioni meno onerose a parità di sicurezza, ma promette piuttosto di rivoluzionare, al pari dell'IA, le strategie aziendali. La principale sfida per le aziende nell'adozione della Blockchain è, quindi, soprattutto di natura strategica. Infatti, il cambio di paradigma necessario ad applicare efficacemente questi nuovi mantra è tale da richiedere non più il semplice adattamento delle

[147] Fonte: Brant Carson, Giulio Romanelli, Patricia Walsh, Askhat Zhumaev, "*Blockchain beyond the hype: What is the strategic business value*", 2018.
[148] Fonte: "*Competitive Advantage, Agglomeration Economies, and Regional Policy",* Michael E. Porter, 1996.

strategie aziendali ma una loro totale ridefinizione dalle fondamenta in ottica digital first. All'innovazione tecnologica scaturita dal fenomeno Blockchain occorre dunque affiancare quella strategica inerente il modello di business aziendale.

Il framework su cui baseremo l'analisi degli impatti della tecnologia Blockchain sulla realtà aziendale può essere rappresentato astrattamente da un tetraedro[149] (*figura 22*).

[149] Fonte: Bagnoli, Bravin, Massaro, Vignotto, "*BusinessModel4.0 - I Modelli di Business vincenti per le imprese italiane nella quarta rivoluzione industriale*", Edizioni Ca' Foscari, Venezia, 2018.

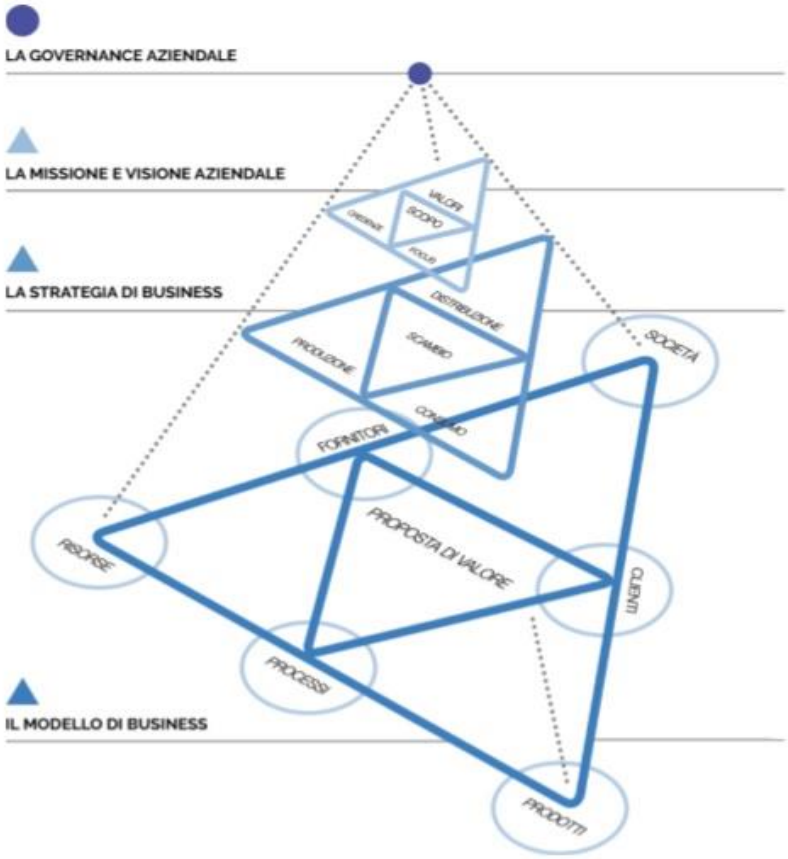

Figura 22. BC e modello di business, strategia aziendale, mission, vision, governance. Fonte: "Gli impatti di IA e di Blockchain sui modelli di business", Strategy Innovation Forum, 2020.

Nel presente paragrafo analizzeremo, dunque, l'impatto presente e futuro della tecnologia BC sui seguenti aspetti: modello di business, strategia aziendale, mission, vision e, infine, governance aziendale.

Prima di procedere a livello di analisi, offriamo di seguito un breve chiarimento relativo ai succitati aspetti alla base del framework aziendale:

⇨ Il **modello di business** rappresenta la logica attraverso cui un'azienda crea valore per sé e per i suoi stakeholders, anche e soprattutto attraverso lo sfruttamento di una nuova tecnologia. Un business model è composto dai seguenti building block, tra loro strettamente interconnessi:

- *fornitori*: soggetti con i quali l'azienda instaura relazioni per l'approvvigionamento di risorse che non produce internamente e/o non ha a disposizione.
- *risorse*: beni economici materiali e immateriali necessari ad alimentare i processi;
- *processi*: sistemi di attività che l'azienda sviluppa per trasformare gli input (risorse) in output (prodotti).
- *prodotti*: offerta con cui l'azienda si presenta sul mercato per soddisfare i bisogni espliciti, latenti o inesistenti dei clienti.
- *clienti*: destinatari dell'output, i quali certificano o meno la validità della proposta di valore dell'azienda.

⇨ La **strategia di business** definisce la posizione competitiva che l'azienda vuole raggiungere e dalla quale si origina il modello di business.

- ⇨ Per **missione** aziendale intendiamo l'identità profonda e immutabile dell'azienda, l'obiettivo complessivo della sua strategia, dunque, lo scopo che informa il modello di business[150].
- ⇨ La **visione** aziendale è, invece, descrizione della situazione futura desiderata per l'azienda: essa riguarda qualcosa che non esiste oggi e che non è mai esistito in precedenza, e ha l'intento di coinvolgere l'intera organizzazione verso il raggiungimento futuro dell'obiettivo.
- ⇨ La **governance**, intesa come perno strutturale di qualsiasi realtà aziendale, esprime le regole e i processi con cui si prendono le decisioni in un'azienda, le modalità con cui vengono decisi gli obiettivi aziendali nonché i mezzi per il raggiungimento e la misurazione dei risultati raggiunti.

3.3.1 L'impatto della Blockchain sui building block del modello di business

È lecito ritenere che la tecnologia Blockchain, in vista della sua fisionomia e anatomia, abbia un impatto significativo sulla gestione dei *fornitori* da parte di un'azienda, alimentando la trasparenza delle transazioni e dei processi di scambio, permettendo di ridurre il rischio di corruzione, tracciando la provenienza degli asset e abilitando l'accesso sicuro ai dati sugli stessi. Le interazioni tra fornitori,

[150] Fonte: "*The Company Mission As a Strategic Tool*", Pearce, 1982.

istituzioni, sistemi e servizi diventano così trasparenti e verificabili in ogni momento del ciclo di vita della risorsa[151]. Alla stessa maniera, grazie alla creazione di piattaforme di scambio sicure, la Blockchain facilita le partnership *peer-to-peer* tra aziende, rafforzando ed espandendo le supply chain[152]. D'altro canto, dato che tutte le transazioni e contratti vengono archiviati in modo non modificabile sulla Blockchain, gli stessi fornitori possono utilizzare questa catena di controllo per dimostrare la propria solvibilità, per il tracciamento della propria identità e reputazione sul mercato[153].

A livello delle *risorse*, la Blockchain permette di creare mercati crittografati in cui le risorse facilmente replicabili, come i dati, diventano scarse. Agendo come un libro mastro distribuito e crittografato, permette infatti di aumentare la trasparenza sulla proprietà delle risorse e dei dati creando un registro completo e inalterabile dei cambiamenti di proprietà[154]. Inoltre, l'integrazione della Blockchain a tecniche di IA permette di identificare in real-time la presenza di attacchi ai dati e richiamare in modo automatico il meccanismo di difesa più appropriato per ogni azienda, aumentando così la sicurezza nella gestione degli asset digitali[155].

---

[151] Fonte: EY, "*Blockchain Technology as a Platform for Digitization. Implications for the Insurance Industry*", 2015.
[152] Fonte: Vida J. Morkunas, Jeannette Paschen, Edward Boon, "*How blockchain technologies impact your business model*", Business Horizons, 2019, vol. 62, issue 3, 295-306.
[153] Fonte: "*The impact of the blockchain on the supply chain: a theory-based research framework and a call for action*", Treiblmaier, 2018.
[154] Fonte: "*Global Blockchain Benchmarking Study*", Hileman, Rauchs, 2017.
[155] Fonte: Hileman *et al*., 2017.

La Blockchain impatta altresì sui *processi* interni all'azienda: grazie alla standardizzazione dei dati, aumenta la velocità di scambio delle informazioni tra dipartimenti e divisioni aziendali, rendendo maggiormente efficienti i processi di scambio e di comunicazione all'interno della stessa impresa[156]. Ciò si riflette nei processi produttivi, dove l'integrazione della Blockchain con tecnologie dell'Internet of Things è in grado di aumentare la disponibilità delle informazioni sullo stato attuale di veicoli e macchinari[157]. L'applicazione della BC, inoltre, porta a migliorare l'affidabilità dei processi di consegna grazie alla capacità di tracciare le certificazioni in tempo reale. Per quanto riguarda i processi di vendita, uno degli elementi resi possibili è l'impiego di *smart contracts*, tramite i quali si stabiliscono transazioni sicure e completamente tracciabili facendo leva sull'immutabilità e l'inviolabilità della tecnologia sottostante: ogni transazione dovrà essere verificata dai partner dell'ecosistema, quindi sarà visibile in tempo reale pur preservando la privacy dell'utente. Automatizzare i contratti e le transazioni porta a ridurre i tempi e i costi nel processo di vendita, a ridurre il rischio di frode e ad aumentare la velocità di scambio delle informazioni con i

[156] Fonte: Du, W.D., Pan, S.L., Leidner, D.E., Ying, W., "*Affordances, experimentation and actualization of FinTech: A Blockchain implementation study*", Journal of Strategic Information Systems, 2018.
[157] Fonte: Treiblmaier,H., 2018, "*The impactofthe Blockchainon the supplychain:a theory-basedresearch frameworkand a call for action*", Supply Chain Management, Vol. 23 No. 6, pp.545–559.

clienti. La sicurezza nei pagamenti aumenta, così come la sicurezza e la privacy nello scambio dei dati[158].

Inoltre, la Blockchain ha un impatto positivo sui *prodotti*, intervenendo nell'autenticazione dei beni scambiati, intesi come oggetto di una transazione commerciale. Se questi beni sono complessi o la loro autenticità non può essere immediatamente convalidata e se il consumo implica elementi percettivi profondi o i valori del marchio correlati sono alti, la necessità di autenticazione è forte, motivo per cui la Blockchain trova ampio spazio di applicazione[159]. Il suo utilizzo nel settore agroalimentare permette ad esempio di conoscere la storia dei prodotti, dalla nascita al consumatore finale, limitando i rischi di contraffazione.

Dal punto di vista dei *clienti* finali, la garanzia di sicurezza e privacy può incoraggiare la condivisione dei dati: la Blockchain restituisce il controllo dei dati nelle mani degli utenti, aumentando la fiducia nella condivisione dei dati e la consapevolezza che questi verranno utilizzati correttamente per fornire una migliore personalizzazione dei prodotti e dei servizi che ricevono[160]. La natura distribuita, il modello cooperativo che impedisce la modifica retroattiva dei dati contenuti nei blocchi e il processo crittografico rendono infatti robusto e affidabile il meccanismo di gestione dei dati, senza l'intervento di intermediari. Grazie a

[158] Fonte: Vida J. Morkunas, Jeannette Paschen, Edward Boon, "*How blockchain technologies impact your business model*", Business Horizons, 2019, vol. 62.
[159] Fonte: Nowiński, W., Kozma, M., 2017, "*How can Blockchain technology disrupt the existing business models?",Entrepreneurial Business and Economics Review*, Vol. 5 No. 3, pp. 173–188.
[160] Fonte: Dinh, T.N., Thai, M.T., 2018, "*AI and Blockchain: A Disruptive Integration*", Computer, Vol. 51 No. 9, pp. 48-53.

queste peculiarità, la Blockchain facilita inoltre l'accesso a mercati target che erano precedentemente inaccessibili, creando nuovi segmenti di clientela fruibili per l'azienda[161]. Le potenzialità di BC rivoluzionano dunque non solo i processi di scambio, bensì le basi stesse delle relazioni di fiducia tra produttori, consumatori e stakeholders.

L'identificazione degli impatti della Blockchain sui singoli building block del modello di business permette di far emergere il contesto operativo e competitivo nel quale le aziende si troveranno ad operare nel prossimo futuro. Il contesto operativo sarà trasformato dalle nuove forme di pagamento, capaci di rivoluzionare il sistema dei trasferimenti di denaro tra aziende a livello internazionale, riducendo i costi, incrementando l'efficienza e rendendo l'intero processo più trasparente, sfidando in tal modo i sistemi di trasferimento interbancario tradizionali[162]. In prima istanza, il sistema dei pagamenti risulterà modificato negli attori, nei mezzi e negli strumenti. In seconda istanza, la Blockchain renderà possibile l'istituzione di una moneta per l'intera comunità umana delegittimando così le banche centrali e quindi gli Stati sovrani. La moneta, infatti, "*non è semplicemente un simbolo, ma un emblema istituito per una comunità in nome di un'istanza di sovranità. Nessuna moneta, a nessun*

[161] Fonte: Morkunas, V.J., Paschen, J., Boon, E., 2019, "*How Blockchain technologies impact your business model*", Business Horizons, "Kelley School of Business, Indiana University", Vol. 62 No. 3, pp.295–306.

[162] Fonte: Vida J. Morkunas, Jeannette Paschen, Edward Boon, "*How blockchain technologies impact your business model*", Business Horizons, 2019, vol. 62.

livello genera automaticamente una comunità. Piuttosto, l'istituzione monetaria presuppone sempre una comunità per la quale avere luogo"[163].

Il contesto competitivo del futuro sarà caratterizzato dalla riduzione dei costi di transazione, mettendo in discussione gli operatori che svolgono funzione di intermediazione[164]. La possibilità di inglobare contratti ad esecuzione automatica e lo sviluppo di internet decentralizzato porteranno all'implementazione di soluzioni che consentiranno l'incontro diretto di domanda ed offerta, migliorando l'efficienza complessiva del sistema competitivo, e spingendo verso lo sviluppo di *Distributed Autonomous Organizations*[165]. In questo contesto, le aziende che basano il proprio vantaggio competitivo sulla possibilità di diventare attori ecosistemici in grado di far incontrare domanda ed offerta vedranno pesantemente messa in discussione la loro stessa utilità.

3.3.2 L'impatto della Blockchain sulla strategia di business

Esiste uno stretto collegamento tra gli impatti della Blockchain sui building block del modello di business e quelli sulla strategia di business. Prima di approfondire gli ultimi è opportuno, tuttavia, affrontare i possibili impatti di BC sulla strategia tecnologica. In linea teorica, si possono distinguere due strategie tecnologiche

[163] Fonte: Amato M., 2010, "*L'enigma della moneta e l'inizio dell'economia*", Feltrinelli.
[164] Fonte: Vida J. Morkunas *et al*., 2019.
[165] Fonte: Vida J. Morkunas *et al*., 2019.

"generiche" e contrapposte: l'una volta ad aumentare l'apertura e la libertà del sistema per consentire il raggiungimento di un equilibrio emergente, l'altra, al contrario, volta ad aumentare la chiusura e il controllo del sistema per consentire il raggiungimento di un equilibrio deliberato[166]. Nello specifico, la prima strategia si caratterizza per il perseguimento di obiettivi quali la decentralizzazione, l'esternalizzazione, l'interoperabilità, la fruibilità, la predizione, l'umanizzazione, la flessibilità e la complessificazione. La seconda si caratterizza, invece, per il fatto di perseguire i contrapposti obiettivi della centralizzazione, internalizzazione, proprietà, sicurezza, reattività, automazione, efficienza e semplificazione.

STRATEGIA TECNOLOGICA	
Aperta e libera	Chiusa e controllata
Decentralizzazione	*Centralizzazione*
Esternalizzazione	*Internalizzazione*
Interoperabilità	*Proprietà*
Fruibilità	*Sicurezza*
Predizione	*Reattività*
Umanizzazione	*Automazione*

[166] Fonte: "*Gli impatti di IA e di Blockchain sui modelli di business*", Strategy Innovation Forum, 2020.

Flessibilità	*Efficienza*
Complessificazione	*Semplificazione*

Figura 23. Tabella riassuntiva delle caratteristiche tra le due diverse accezioni di strategia tecnologica. Fonte: elaborazione dell'autore.

La Blockchain, come più volte sottolineato, è una tecnologia che consente di archiviare i dati in modo sicuro, verificabile e permanente attraverso un registro digitale aperto e distribuito. Tale registro adotta un nuovo modo per:

- *valorizzare*, ossia attribuire valore a dati non duplicabili e quindi dotati di valore economico, quali ad esempio le criptovalute;
- *interagire*, ossia mettere in relazione diretta soggetti senza una terza parte che funga da attore centrale;
- *fidarsi*, ossia fare affidamento su dati non alterabili e non cancellabili;
- *negoziare*, ossia sviluppare contratti che si eseguano automaticamente al verificarsi di determinate condizioni.

Nella figura sottostante sono riportate le frequenze nel perseguimento dei diversi e contrapposti obiettivi strategici (evidenziati nella *figura 23*) da parte della tecnologia Blockchain.

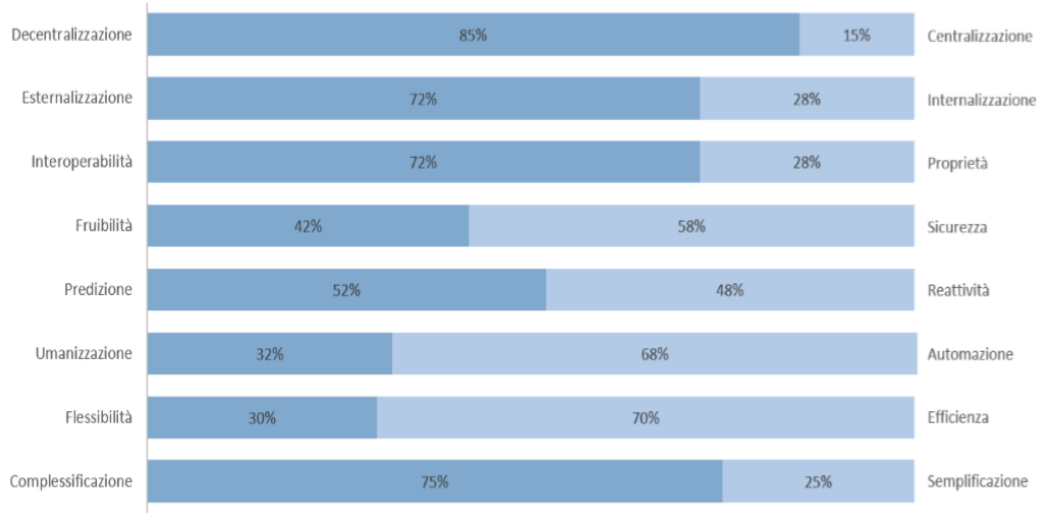

Figura 24. Perseguimento degli obiettivi delineati nelle due diverse accezioni di strategia tecnologica da parte della Blockchain. Fonte: "Gli impatti di IA e di Blockchain sui modelli di business", Strategy Innovation Forum, 2020.

In primo luogo, l'85% dei potenziali impatti della Blockchain sembra incoraggiare strategie tecnologiche volte ad aumentare la decentralizzazione (a scapito della centralizzazione) e il 72% l'esternalizzazione (contro l'internalizzazione). Questo risultato è coerente con la natura stessa della Blockchain che nasce esattamente come sistema di gestione distribuita di dati e processi, ed esegue le sue funzioni demandando controllo ed esecuzione ad una rete di soggetti esterni alle singole organizzazioni. Per lo stesso motivo, l'interoperabilità prevale con il 72% sulla proprietà, essendo un requisito imprescindibile della tecnologia per abilitare i processi di condivisione e distribuzione delle informazioni che sono alla base del funzionamento dei sistemi

Blockchain. Può invece stupire che non emerga una particolare polarizzazione di questa tecnologia su strategie orientate alla sicurezza, essendo il peso del 58% di quest'ultima sostanzialmente bilanciato con il 42% della fruibilità. A seguito di un'analisi più accurata, tuttavia, questa peculiarità diventa comprensibile: va considerato che la tecnologia Blockchain può essere estremamente efficace sia per garantire integrità, certificabilità e non-ripudiabilità dei dati, sia per fare in modo che questi, attraverso la rete dei nodi coinvolti, siano resi pubblici, fruibili e facilmente accessibili. In un certo senso, infatti, la forza della Blockchain sta proprio nella relazione simbiotica fra condivisione pubblica su larga scala e certificazione distribuita del dato. Una situazione altrettanto bilanciata è osservabile tra la caratteristica della predizione (52%) e quella della reattività (48%): in questo caso il bilanciamento è più propriamente dovuto ad una sostanziale neutralità della tecnologia in esame rispetto a questi temi strategici. Infatti, la Blockchain non è una tecnologia focalizzata sull'ottenimento di risposte efficaci dall'analisi dei dati, ma piuttosto sulla conservazione, distribuzione e gestione efficiente ed automatizzata dei dati stessi. Anche quest'ultimo aspetto risulta pienamente confermato dall'analisi della letteratura, che ci restituisce appunto un deciso orientamento strategico da parte della BC verso i temi dell'automazione (68%) e dell'efficienza (70%). Infine, per quanto possa risultare illogico, l'introduzione della Blockchain in ambito aziendale comporta tendenzialmente una complessificazione (75%) piuttosto che una semplificazione

(25%) dei sistemi e dei processi aziendali. Questo fenomeno va interpretato osservando che, se da un lato la Blockchain mette a disposizione strumenti potenti per certificare e gestire in modo sicuro dati e transazioni, nel contempo costringe le organizzazioni a ripensare ai propri processi per trarne un reale vantaggio. A sua volta questo può comportare la necessità di gestire appropriatamente nuovi tipi di informazione che prima erano semplicemente non disponibili. Per questo motivo, come per la maggior parte delle tecnologie digitali, l'adozione della Blockchain come strumento tecnologico non può prescindere dalla rimodulazione dei processi interni e, con ogni probabilità, degli stessi modelli di business.

L'identificazione degli impatti che la Blockchain può generare sui singoli building block del modello di business (*par. 3.3.1*) ha permesso di far emergere anche gli impatti diretti e indiretti della tecnologia stessa a livello dell'intero modello di business e, quindi, a livello di strategia aziendale. Infatti, i modelli di business tradizionali nei settori esistenti possono essere innovati grazie al ricorso diretto alla Blockchain, ma anche "copiando" i modelli di business innovativi nei settori emergenti che la Blockchain stessa ha portato a creare. Nel primo caso, con riferimento specifico al settore retail, l'avvento della Blockchain permette di realizzare marketplace decentralizzati che rendono possibile la compravendita di prodotti tramite la validazione delle transazioni da parte dei partecipanti della rete BC, e quindi l'eliminazione della funzione di intermediazione svolta da

piattaforme centralizzate quali Amazon ed Ebay[167]. Tutto ciò permette alle imprese di distribuzione esistenti di passare dal modello di business "Marketplace" a quello definibile "Decentralized Applications" basato su una rete decentralizzata per il commercio *peer-to-peer* online senza commissioni sulle compravendite, restrizioni sulle categorie di prodotti scambiati, account da creare, rivelando solo le informazioni personali desiderate e ricorrendo a criptovalute[168]. Più probabilmente, porterà all'affermazione di imprese di distribuzione nuove, come ad esempio OpenBaazar, che collegano, appunto, direttamente acquirenti e venditori. Nel caso di impatto indiretto della BC a livello di modello di business, è osservabile come il tradizionale business model "Markteplace", inizialmente adottato dai Blockchain providers, quali ad esempio MyEtherWallet[169], sia stato innovato dalla nota piattaforma Ethereum, che lo ha modificato basandolo sugli "Utility token", che danno diritto ad acquistare la capacità di calcolo messa a disposizione dai partecipanti alla rete Blockchain di Ethereum[170]. Questo nuovo ed emergente modello di business è stato poi a sua volta copiato da imprese operanti nei settori esistenti quali, ad esempio, Lympo. Esso rappresenta un ecosistema alimentato da dati di fitness e benessere generati e controllati

[167] Fonte: Tumasjan, A., Beutel, T., 2019, "*Blockchain-Based Decentralized Business Models in the Sharing Economy: A Technology Adoption Perspective*", Business Transformation through Blockchain, pp. 77–120.
[168] Fonte: Tumasjan *et al*., 2019.
[169] MyEtherWallet è un'nterfaccia utente open source gratuita che aiuta a interagire con la Blockchain di Ethereum, consentendo di generare portafogli, interagire con contratti intelligenti, e così via. Fonte: Nexo, 2018, "*Nexo: The World's First Instant Crypto-baked Loans*", White Paper.
[170] Fonte: Singh, N., 2018, "*Top 7 Blockchain Business Models That You Should Know About*".

dall'utente, il quale viene ricompensato con token "LYM" al conseguimento di obiettivi di stile di vita sano.

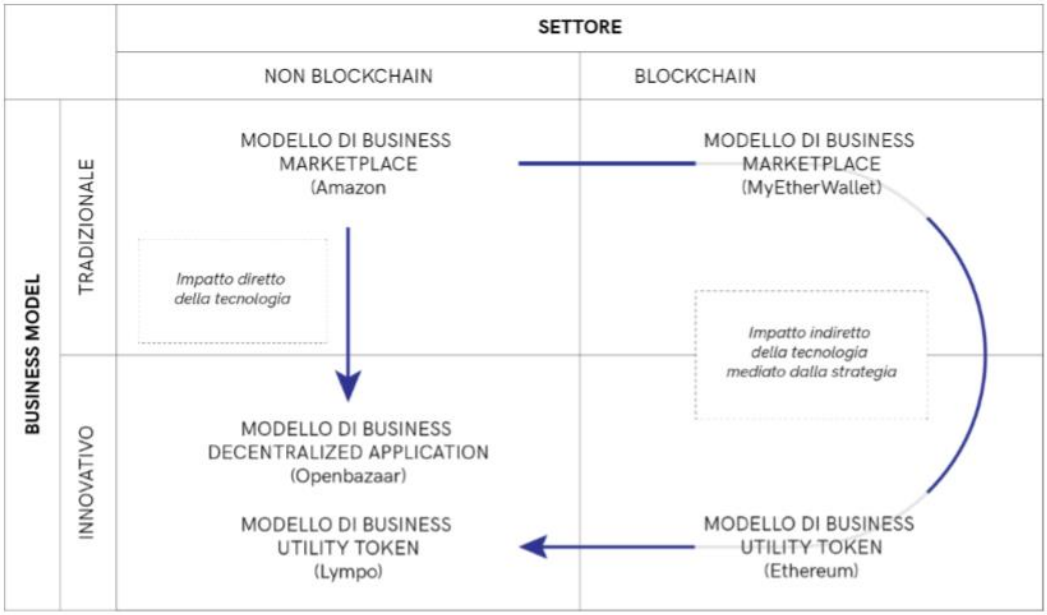

Figura 25. Impatto diretto e indiretto della BC sui principali modelli di business. Fonte: "Gli impatti di IA e di Blockchain sui modelli di business", Strategy Innovation Forum, 2020.

3.3.3 L'impatto della Blockchain sulla missione, visione e governance aziendale

Come più volte sottolineato nel corso della trattazione, la Blockchain consente di acquisire dati pubblicamente osservabili che, in quanto organizzati in forma strutturata attraverso un sistema di archiviazione sicuro, crittografato, distribuito, e immutabile, assumono carattere di unicità e non duplicabilità. Affinché i dati pubblici, ma unici, vengano liberamente scambiati, è necessario possedere una conoscenza architetturale, funzionale alla definizione delle regole attraverso cui

gli attori del network inseriscono nuove informazioni e validano quelle aggiunte dagli altri operatori nella catena. La conoscenza richiesta per lo sviluppo di tali soluzioni si concentra, pertanto, nello sviluppo di algoritmi di consenso (regole per l'inserimento dei dati accettati da tutti i partecipanti al network). La solidità del sistema di archiviazione dipende dalla dimensione dello stesso e facilita pertanto lo sviluppo di economie di network, dove le reti più ampie, cioè con il maggior numero di partecipanti, vincono su quelle più ridotte: infatti, la crescita dimensionale del network ne incrementa la solidità ed elimina la necessità di preporre figure intermedie per il controllo del sistema. E la fiducia nella solidità del sistema consente di automatizzare gli scambi grazie all'introduzione degli *smart contract*. Ne consegue una progressiva riduzione dei costi di transazione che spinge verso situazioni di concorrenza perfetta, in cui aziende atomistiche fatte di liberi professionisti dialogano tra loro[171].

A fronte di tali premesse, emerge chiaramente che la Blockchain presenta un approccio alla gestione della complessità basandosi sul meccanismo della fiducia e, in conformità a ciò, un approccio alla gestione della conoscenza di tipo distribuito[172]. Conoscenza e complessità si rincorrono in maniera costante, con la prima che cerca di ridurre la seconda; d'altro canto, un sistema complesso ha

[171] Fonte: "*Gli impatti di IA e di Blockchain sui modelli di business*", Strategy Innovation Forum, 2020.

[172] Tumasjan,A., Beutel, T., 2019, "*Blockchain-BasedDecentralizedBusiness Modelsin the SharingEconomy:A Technology Adoption Perspective*", Business Transformation through Blockchain, No. July, pp. 77–120.

bisogno di sempre più conoscenza che, al suo accrescere, fa aumentare la complessità del sistema stesso. Metaforicamente, è possibile generare un diagramma cartesiano caratterizzato da un asse verticale, definito *asse della conoscenza*, e uno orizzontale, definito *asse della complessità*[173]. Coerentemente con quanto finora affermato, l'asse della conoscenza indicherebbe graficamente il concetto di "distribuzione", l'asse della complessità, invece, quello di "fiducia": entrambe le connotazioni fanno capo allo spirito della Blockchain.

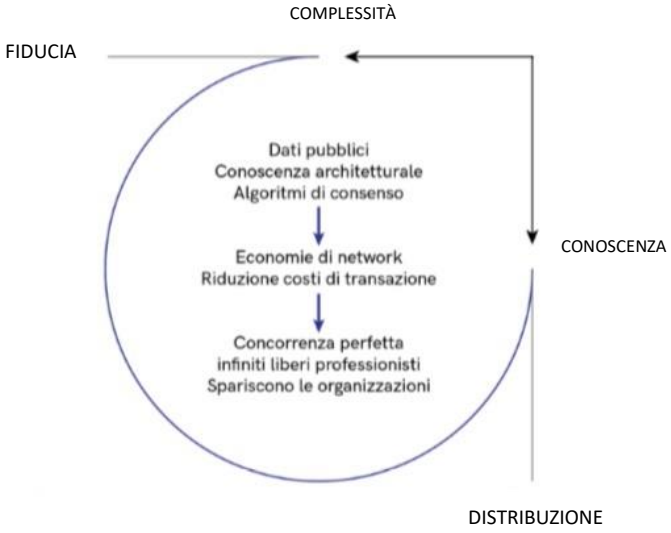

Figura 26. BC tra fiducia e decentralizzazione. Fonte: "Gli impatti di IA e di Blockchain sui modelli di business", Strategy Innovation Forum, 2020.

[173] Tumasjan,A., Beutel, T., 2019, "*Blockchain-BasedDecentralizedBusiness Modelsin the SharingEconomy:A Technology Adoption Perspective*", Business Transformation through Blockchain, No. July, pp. 77–120.

Sinteticamente, la Blockchain si basa su dati pubblici, si fonda su una conoscenza architetturale e su algoritmi di consenso, cerca di raggiungere economie di network, permette la riduzione dei costi di transazione. E sulla base di tali peculiarità, si identificherebbe, per opera della Blockchain, uno scenario futuro, definibile "Gig economy", che vedrebbe l'avvento di una situazione di concorrenza perfetta caratterizzata dalla presenza di infiniti liberi professionisti e, quindi, dalla sparizione delle singole organizzazioni[174]. Pertanto, la soluzione da perseguire, in termini grafici, è evitare di raggiungere il punto di equilibrio statico in basso a sinistra del diagramma (supremazia di un sistema totalmente basato sulla "fiducia distribuita"), a favore di un equilibrio dinamico che persegua simultaneamente una "fiducia distribuita" e, agli antipodi, un "controllo centralizzato", disegnando una curva a "infinito"[175]. Questa soluzione sembra anche quella che permette alle imprese di creare nel breve termine un vantaggio competitivo sostenibile. In conclusione, è impossibile definire una missione, una visione e una governance aziendale valida per tutte le imprese, ma è possibile affermare che tutte devono porsi il problema di come non sparire nel medio termine per l'affermazione di un sistema totalmente basato sulla "fiducia distribuita" (quindi sulla Blockchain) o sul "controllo centralizzato", e di come

[174] Fonte: "*Gli impatti di IA e di Blockchain sui modelli di business*", Strategy Innovation Forum, 2020.
[175] Fonte: Tumasjan,A., Beutel, T., 2019, "*Blockchain-BasedDecentralizedBusiness Modelsin the SharingEconomy:A Technology Adoption Perspective*", Business Transformation through Blockchain, No. July, pp. 77–120.

generare nel breve termine un vantaggio competitivo sostenibile, ricercando, quindi, un equilibrio dinamico efficiente.

CAPITOLO 4

AMBITI APPLICATIVI DELLA TECNOLOGIA BLOCKCHAIN

L'obiettivo del presente capitolo è quello di illustrare una pluralità di effettive e potenziali applicazioni settoriali della tecnologia Blockchain, a dimostrazione del crescente interesse maturato nei confronti di quest'ultima anche al di fuori dell'ambito *finance*. L'analisi inizia con la presentazione dei principali investimenti in essere e delle prospettive di crescita dei progetti avviati e prosegue poi con una disamina dei principali settori di impiego.

4.1 Aspetti normativi: progetti avviati e fondi stanziati

Quanto esaminato nei capitoli precedenti in riferimento all'anatomia e alla fisionomia della tecnologia Blockchain trova immediato riscontro in tantissimi aspetti della vita quotidiana, sia dei singoli soggetti che delle imprese.

Le nuove tecnologie offerte dalla digitalizzazione, quali Blockchain, Internet of Things (IoT), Intelligenza Artificiale (IA), sono attualmente supportate nello

sviluppo dalle Istituzioni Europee ed Italiane. Recentemente la Commissione UE ha promosso una iniziativa denominata "European Blockchain Partnership" che ha lo scopo di creare una piattaforma europea, basata sulla tecnologia Blockchain, finalizzata ai servizi pubblici, alla quale ha aderito anche l'Italia il 27 settembre 2018[176]. Il Decreto Semplificazioni 2019 con l'art. 8 ter, pubblicato sulla Gazzetta Ufficiale del 12 febbraio 2019 Serie Generale n.36, finalmente, introduce in Italia l'inquadramento giuridico relativo alla *Distributed Ledger Tecnology* e agli *smart contract* che risulta completato dalle Norme Antiriciclaggio dell'Unione Europea, Direttiva (UE) 2018/843, e dal "Rapporto sulla stabilità finanziaria n. 1/2018" del 27 aprile 2018 della Banca d'Italia[177].

Le norme citate, base di partenza per la definizione di quanto sarà necessario per il riconoscimento giuridico delle criptovalute, sono esaustive per dar corso allo sviluppo della Blockchain in Italia per le transazioni di valori, o meglio, dei cosiddetti asset digitali, nonché per il riconoscimento giuridico dell'identificazione elettronica e servizi fiduciari per le transazioni elettroniche così come previsto dall'art.41 del Regolamento UE n. 910/2014 e, pertanto, dell'attuazione degli *smart contract*.

La Legge di Bilancio 2019 art.19 ha istituito un fondo per favorire lo sviluppo delle tecnologie e delle applicazioni di intelligenza artificiale, Blockchain e

[176] Fonte: "*Blockchain: disruption and opportunity*", Natalia Maslova, July 2018.
[177] Fonte: "*Blockchain, le principali normative nazionali al mondo*", Angelo Alù, 2019.

Internet of Things, meglio noto come “fondo blockchain”: la dotazione ammonta a 15 milioni di euro per ciascuno degli anni 2019, 2020 e 2021. Nello specifico, la Manovra 2019 è destinata a finanziare:

a) progetti di ricerca e innovazione da realizzare in Italia ad opera di soggetti pubblici e privati, anche esteri, nelle aree strategiche per lo sviluppo dell’IA, della Blockchain e dell’IoT, funzionali alla competitività del paese;
b) sfide competitive per il raggiungimento di specifici obiettivi tecnologici e applicativi;
c) il supporto operativo ed amministrativo alla realizzazione di quanto previsto ai punti precedenti, al fine di valorizzarne i risultati e favorire il loro trasferimento verso il sistema economico produttivo, con particolare attenzione alle piccole e medie imprese.

Inoltre, tra le più importanti e recenti iniziative c’è proprio il succitato lavoro della EBP indirizzato allo sviluppo di una European Blockchain Services Infrastructure (EBSI), un’infrastruttura europea che, partendo dalla considerazione che “la Blockchain è globale o non è Blockchain”, si è data l’obiettivo di sviluppare e diffondere le *capabilities* che permettono di garantire l’apertura, l’interconnessione, la interoperabilità[178]. Esattamente ciò che serve alle imprese

[178] Più precisamente l’infrastruttura europea di servizi Blockchain – avviata a febbraio 2019 – costituisce un’iniziativa congiunta della Commissione europea e del partenariato europeo

per scegliere di investire in Blockchain. Molto significativo che su questi temi ci sia un forte impegno proprio dell'Italia.

Il quadro di riferimento si compone anche grazie all'indiscutibile iniziativa di alcuni paesi come la Svizzera che sui temi della nuova regolamentazione della *tokenizzazione* per i mercati finanziari sta facendo da apripista e sta gettando le basi tanto per la costruzione di progetti sperimentali quanto per disporre di quelle esperienze che consentono poi di scrivere le regole vere e proprie. Intanto, anche con le competenze e l'iniziativa di tanti italiani, la Svizzera detta il ritmo con la prima regolamentazione del mercato dei capitali firmato dalla Swiss Blockchain Federation[179].

A livello di iniziative internazionali un ruolo importante è svolto dall'OCSE, che si concretizza in particolare sui temi della certificazione di provenienza garantita dei prodotti, ovvero su un asset fondamentale per il nostro paese e per le PMI in particolare.

Blockchain (EBP) per fornire servizi pubblici transfrontalieri a livello dell'UE utilizzando la tecnologia Blockchain. Fonte: "*European Blockchain Service Infrastructure (EBSI), che cos'è e quali sono i vantaggi*", Gianluigi Torchiani, 2019.

[179] L'associazione Svizzera presenta un manuale con le linee guida per gli emittenti di *digital equity* e dei relativi *token* con una particolare attenzione alle piccole e medie imprese. Il punto di attenzione di questo documento è nella consapevolezza che i *digital token* possono aprire anche alle imprese di minori dimensioni la possibilità di digitalizzare il capitale, emettere certificati, *equity*, obbligazioni nel rispetto di framework normativi. In questo scenario si parla di asset che sono trasferibili in pochi secondi con la possibilità di dare vita a un mercato secondario per permette a queste imprese di accedere a nuove fonti di finanziamento. La Swiss Blockchain Federation con queste linee guida punta a consolidare e rafforzare il ruolo della Svizzera come mercato di riferimento per queste operazioni e lo vuole fare mettendo in evidenza che si tratta di percorsi che non sono esclusivi per le sole grandi imprese. Fonte: Mauro Bellini, "*La roadmap verso i capital market del futuro secondo la Swiss Blockchain Federation*", 2020.

Pertanto, è possibile affermare che lo sviluppo e l'applicazione della Blockchain e dell'innovazione digitale godono oggi del supporto e del sostegno da parte delle Istituzioni mediante le normative sopra descritte.

4.2 Ambiti applicativi della tecnologia

Blockchain è sinonimo di sicurezza nello scambio di asset, inviolabilità del registro decentralizzato, efficienza ed economicità delle transazioni. Non è difficile credere quindi che gli ambiti applicativi della presente tecnologia siano molti: in alcuni di questi sono già implementate soluzioni che poggiano su una struttura Blockchain, in altri la fase di sperimentazione è appena cominciata.

Secondo una ricerca sviluppata dall'Osservatorio Blockchain del Politecnico di Milano nel 2018, gli ambiti applicativi della Blockchain in Italia possono esser distinti in due categorie:

1. Quelli appartenenti all'area del **finance**, che include, tra i tanti, Payments, Capital Markets, Compliance, Trade Finance, Insurance, etc.;
2. Quelli appartenenti all'aerea del **non finance**, ossia tantissimi altri settori, quali Internet of Things, Smart Contracts, Data Storage, Tracking, Supply-Chain Management, Health Care, Public Administration, etc.

Da questa prima analisi si evince che i potenziali ambiti di impiego della tecnologia, così come evidenziato dagli esperti del Politecnico, sono molti e buona parte di essi non appartiene all'area finanziaria.

Per avere qualche informazione aggiuntiva relativa al livello di interesse che le aziende hanno maturato negli anni nei confronti della Blockchain, inoltre, si riporta l'indagine[180] che la multinazionale dei servizi PwC condusse coinvolgendo circa 600 amministratori delegati di aziende di 15 Paesi diversi, Italia inclusa. Dall'indagine emerse che l'84% delle aziende era coinvolto in progetti di ricerca sulla Blockchain: in particolare, il 20% di queste stava studiando la tecnologia, il 32% era già in fase di sviluppo, il 10% lavorava all'avviamento di progetti pilota, il 15% stava implementando soluzioni e il 7% aveva bloccato, per varie ragioni, progetti già avviati. Solo il 14% dichiarò di non aver alcun coinvolgimento previsto in questo ambito.

Figura 27. Percentuale di aziende coinvolte nella ricerca e nell'applicazione della tecnologia Blockchain. Fonte: PwC Global Blockchain Survey, 2018.

[180] Fonte: PwC Global Blockchain Survey, 2018.

Inoltre, interessante è la chiave di lettura proposta nel 2018 da un'altra nota società leader nella consulenza, Capgemini, secondo cui le tre fasi cruciali nello sviluppo della tecnologia Blockchain possono essere così riassunte:

- Consapevolezza: iniziata nel 2011 è tuttora in corso. Le imprese e le organizzazioni stanno cercando di capire e di sviluppare conoscenza a proposito della tecnologia;
- Sperimentazione: secondo Capgemini, essa è iniziata nel 2017 e durerà sino al 2020. Le imprese e le organizzazioni lavorano per creare competenze, forme di collaborazione, ideare nuovi consorzi, con l'obiettivo di comprendere appieno le potenzialità e le criticità della Blockchain;
- Trasformazione: cominciata nel 2019, ci accompagnerà almeno sino al 2025. In questo arco temporale la Blockchain trasformerà le modalità di relazione, di integrazione e di collaborazione, portando innovazione a più livelli (di tecnologia, di data management, di governance, etc.).

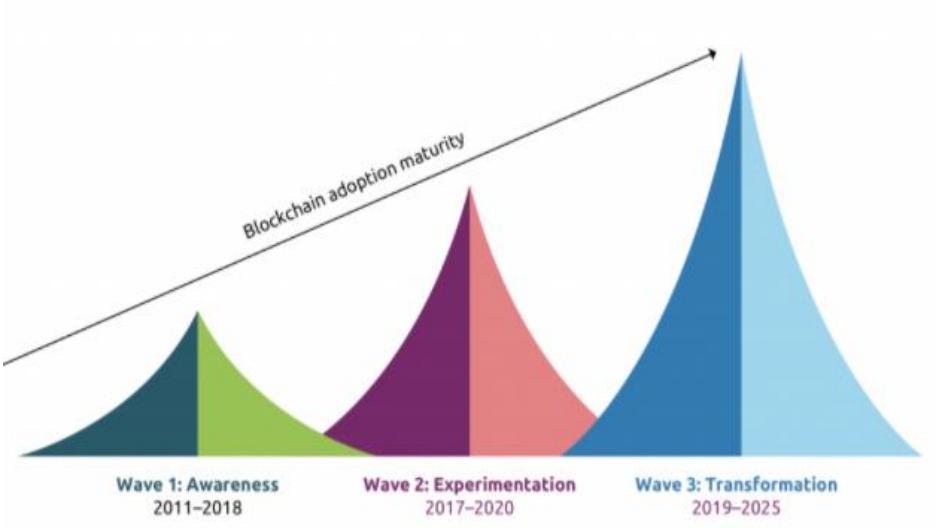

Figura 28. Fasi di maturità della tecnologia BC secondo Capgemini. Fonte: Capgemini, 2018.

Inoltre, secondo la nota società di consulenza Deloitte, la quale ha realizzato nel 2020 un'indagine simile a quella condotta da PwC, ad oggi sono stati investiti oltre un biliardo di dollari nella Blockchain e si contano più di centoventi start-up basate su questa tecnologia. Al suo terzo anno, il Global Blockchain Survey di Deloitte[181] rivela un'avvincente evoluzione della Blockchain da tecnologia sperimentale e dirompente a vera priorità strategica per le organizzazioni. Gli intervistati hanno indicato un aumento del *sentiment*, degli investimenti e dell'approvvigionamento per le iniziative Blockchain. Per la prima volta

[181] Deloitte ha condotto l'indagine tra il 6 febbraio 2020 e il 3 marzo 2020, intervistando un campione di 1.488 dirigenti e professionisti senior in 14 paesi e territori (Brasile, Canada, Cina, Germania, Irlanda, Israele, Messico, Singapore, Sud Africa, Svizzera, Emirati Arabi Uniti, Regno Unito e Stati Uniti). Fonte: Deloitte's 2020 Global Blockchain Survey.

l'indagine approfondisce il ruolo e l'evoluzione degli asset digitali. Tra i principali risultati dell'indagine:

- il 39% degli intervistati globali ha già incorporato la Blockchain nella produzione. Si tratta di un aumento significativo rispetto al 23% dello scorso anno.
- il 55% delle organizzazioni vede la Blockchain come una priorità strategica assoluta, contro il 53% del 2019 e il 43% del 2018.
- l'89% degli intervistati ritiene che le risorse digitali saranno molto importanti per il proprio settore nei prossimi tre anni.
- L'82% degli intervistati ha affermato di assumere personale con esperienza nella Blockchain o intende farlo entro i prossimi 12 mesi, rispetto al 73% dello scorso anno.
- l'83% ha indicato che le proprie aziende perderanno un vantaggio competitivo se non adottano la Blockchain (contro il 77% nel 2019).
- il 70% definisce "molto" o "piuttosto" veloce il ritmo del cambiamento normativo relativo alla Blockchain e alle soluzioni di asset digitali.

È intuibile pertanto che si stanno verificando maggiori progressi nelle iniziative Blockchain su larga scala, inclusa l'infrastruttura finanziaria basata su Blockchain per semplificare il movimento di denaro globale, nonché la tecnologia di registro distribuito per la finanza commerciale e le piattaforme track-and-trace abilitate per Blockchain. "*Sebbene una volta la Blockchain fosse classificata come un*

esperimento tecnologico, ora rappresenta un vero agente di cambiamento che sta interessando l'intera organizzazione: come molte tecnologie dirompenti, si è evoluto da un approccio semplicemente promettente e potenzialmente rivoluzionario a una soluzione ormai integrale per l'innovazione organizzativa"[182]. Il sondaggio di quest'anno, infatti, suggerisce che la Blockchain è saldamente radicata nel pensiero strategico delle organizzazioni in tutti i settori.

Proseguiamo la trattazione analizzando, di seguito, i diversi ambiti applicativi in cui la Blockchain può comportare miglioramenti rispetto alle situazioni in essere, con la possibilità di ridefinire i rapporti tra produttori e consumatori/utilizzatori. L'ordine in cui sono proposti i vari settori di impiego segue una logica gerarchica che parte dalle aree storicamente più interessate dalla tecnologia, cioè nei confronti delle quali essa ha già permesso di implementare soluzioni di successo, e prosegue verso quelle in cui le potenzialità sono ancora oggetto di studio e non ancora alla portata di tutti i player.

4.2.1 Banche e finance

L'area finance è sicuramente il primo settore di impiego della tecnologia Blockchain: per banche e istituti finanziari sta diventando quasi indispensabile accaparrarsi una posizione di prima linea all'interno di tale mercato, che assicura

[182] Fonte: Deloitte's 2020 Global Blockchain Survey.

la velocità e l'affidabilità delle transazioni ed elimina la necessità di un ente super partes che si fa garante dell'autenticità delle operazioni. Proprio per questo tra i principali investitori che si muovono nell'ecosistema Blockchain troviamo banche operanti a livello mondiale. L'approccio da esse utilizzato si può dividere in quattro grandi linee d'azione[183]:

1. Sviluppo interno di Blockchain per la creazione di Private Ledger o piattaforme di money transfer per garantire maggior rapidità e sicurezza nelle transazioni ai propri clienti;
2. Individuazione di partnership con imprese specializzate nella Blockchain per il mondo bancario allo scopo di dare vita a progetti di collaborazione e disporre delle competenze necessarie che l'istituto non possiede internamente;
3. Open innovation con investimenti in start-up o con acquisizioni di imprese che possono apportare competenze e nuove soluzioni;
4. Adesione a grandi consorzi sia di tipo bancario sia cross-sector per accelerare lo sviluppo disponendo di standard condivisi.

Un recente report prodotto da Acta Fintech[184], società di comunicazione e consulenza operante nel settore Fintech e Blockchain, ha fatto luce sull'attuale stato di adozione della presente tecnologia nel settore bancario, prendendo in

[183] Fonte: "*Blockchain e Governance: gli ambiti applicativi nell'Impresa 4.0 con le DLT*", Mauro Bellini, 2018.
[184] Fonte: Acta Fintech, "*Blockchain Banking*", 2020.

esame la scena nazionale ed internazionale. Alcuni degli impieghi principali della Blockchain nel mondo bancario riguardano la ricerca di maggiore sicurezza degli accordi attraverso gli *smart contract*, la gestione dell'Identità Digitale, il raggiungimento di una maggior trasparenza nella gestione dei dati, la *tokenizzazione* di asset fisici ed il trasferimento di fondi cross-border[185].

Figura 29. Implementazione della BC nel settore bancario. Fonte: Acta Fintech, "Blockchain Banking", 2020.

Tra gli esempi più interessanti presentati da Acta Fintech nel documento emerge il caso di Hype: la carta Hype è un prodotto del Gruppo Banca Sella, prima realtà in Italia ad offrire un sistema di pagamenti e-commerce già dal 1997. La sua nuova creazione è la carta ricaricabile Hype, dotata di IBAN per effettuare e ricevere pagamenti. Da un'indagine condotta da Hype su un campione rappresentativo

[185] Fonte: "*Blockchain Banking*", Acta Fintech, 2020.

della propria base utenti, è emerso che ben il 13,5% dei clienti desidera la possibilità di acquistare e scambiare criptovalute[186]. Per questo motivo, in collaborazione con la start-up italiana Conio, Hype ha sviluppato un sistema che consente ai propri clienti l'acquisto di Bitcoin. Il trading viene condotto tramite la piattaforma HYPE dell'azienda, e la banca funge da intermediario per mitigare potenziali rischi per la sicurezza.

Proseguendo con gli esempi di applicazione della tecnologia da parte di banche e istituti finanziari del nostro Paese, nel 2018 UniCredit ha annunciato di aver completato con successo la sua prima transazione commerciale in Italia eseguita con la tecnologia Blockchain[187].

Anche Mediolanum rientra tra gli esempi citati nel report. Con l'utilizzo di Blockchain Ethereum e la conseguente pubblicazione dell'*hash* del documento sul sito istituzionale della Banca[188], Mediolanum ha condotto con successo la certificazione dell'immodificabilità della Dichiarazione Non Finanziaria (DNF). L'adozione di questo processo di notarizzazione rappresenta un'ulteriore

[186] Fonte: "*Blockchain Banking*", Acta Fintech Srl, 2020.

[187] UniCredit nell'Agosto 2018 annuncia di aver completato con successo la sua prima transazione internazionale tramite la piattaforma di trade finance basata su tecnologia blockchain *we.trade*. Fonte: "*Blockchain Banking*", Acta Fintech Srl, 2020.

[188] L'*hash* di un documento è una stringa di testo univoca che è stata generata a partire dal file e ne rappresenta il contenuto. Se l'*hash* viene registrato su una Blockchain permissionless (pubblica), decentralizzata, sicura e robusta come quella di Ethereum, può essere consultato e confrontato con l'*hash* crittografico del documento in possesso degli utenti, in modo da verificare che il suo contenuto sia proprio quello utilizzato per generare l'*hash* memorizzato. Fonte: "*Blockchain Banking*", Acta Fintech Srl, 2020.

conferma dell'impegno della banca nel rendere noto a tutti gli stakeholder impegni, azioni e performance in ambito economico, sociale e ambientale[189].

In via conclusiva, all'interno dell'ambito finance i pagamenti e trasferimenti di denaro gestiti tramite una logica decentralizzata sarebbero tra le funzioni più apprezzate da diversi istituti di credito, in quanto permetterebbero alle banche di poter velocizzare notevolmente le operazioni di routine che tutt'ora comportano una componente di attività burocratica e time-consuming ingente. Inoltre, la garanzia di inviare dati in maniera corretta, verificando l'autenticità del mittente e del destinatario, è un'altra funzione reputata indispensabile per il buon funzionamento di un istituto di finanziamento.

4.2.2 Assicurazioni

Sebbene secondo diverse fonti sia annoverabile all'interno dell'ambito finance, il settore assicurativo può, secondo altri, essere analizzato singolarmente. Indiscutibile l'interesse che si sta sviluppando all'interno di questo ambito attorno al tema Blockchain. Come evidenziato da uno studio condotto da Ernst & Young nel 2017, un aspetto in cui la Blockchain può positivamente intervenire in questo

[189] "*Con orgoglio ci annoveriamo tra le prime banche italiane ad utilizzare i servizi di notarizzazione offerti dalla Blockchain, che significa contemporaneamente garantire l'autenticazione del documento, quindi la sua immodificabilità e irripudiabilità in un'ottica di trasparenza nei confronti di tutti i nostri stakeholder*". Fonte: Oscar Di Montigny, Banca Mediolanum.

settore è proprio quello relativo all'accesso in tempo reale ai dati e ai mutamenti degli stessi, che vengono poi elaborati, adottando strategie di Big Data Analytics, in modo tale da poter offrire al cliente servizi e prodotti che meglio si adattano alle sue necessità.

Una delle applicazioni più dirompenti nel settore è stata Fizzy, un servizio di assicurazione intelligente proposto da Axa, accessibile anche da smartphone[190]. Esso permette al cliente il rimborso automatico in caso di ritardo di un volo superiore alle due ore. Quando si acquista un biglietto, Fizzy registra la transazione sulla Blockchain Ethereum. Il contratto diventa così non modificabile, come i termini dell'accordo. Il servizio è collegato al database mondiale dei voli, così Fizzy può rilevare all'istante i ritardi e inviare automaticamente l'indenizzo ai clienti.

Recentemente, la startup Stratumn, la società di consulenza Deloitte e il fornitore di servizi Lemonway hanno presentato "LenderBot", una micro-assicurazione abilitata alle tecnologie Blockchain. Permettendo di sottoscrivere micro-assicurazioni personalizzate persino chattando tramite l'App Messenger di Facebook, tale progetto elimina la necessità di una terza parte garante del contratto sottoscritto[191].

---

[190] Fonte: "*Blockchain, che cos'è e a cosa serve: dal supermercato alle polizze, come funziona nella vita quotidiana*", Chiara Sottocorona, 2019.

[191] Fonte: "*Blockchain: i benefici concreti e le applicazioni più promettenti per 27 settori*", Mauro Bellini, 2019.

4.2.3 Agrifood

Nel capitolo 2 della presente trattazione è stato sottolineato come, durante una transazione che avviene sulla Blockchain, tramite il *time-stamping* viene marcato ogni blocco di transazioni con data e ora: l'*hash della testa del blocco*, pertanto, si arricchisce di tali informazioni. Se l'operazione coinvolge il trasferimento di una certa quantità di moneta virtuale, come Bitcoin, la storia di questa verrà aggiornata, in modo indelebile, con i dati di ogni scambio avvenuto. Se al posto della moneta si pensa di "trasferire" un kilogrammo d'uva, per esempio, si ha, allo stesso modo, l'opportunità di tracciare tutta la storia dell'alimento, dalla sua raccolta al tavolo del ristorante, e diventa così informazione accessibile e visibile a tutti gli attori della supply-chain.

Ecco che i benefici della Blockchain risultano particolarmente rilevanti per l'industria di trasformazione e per tutte le attività fortemente legate alla certificazione, come quelle del settore alimentare, appunto. Chiunque appartenga alla filiera, dal produttore di materia prima al provider logistico, può aggiungere informazioni preziose alla storia del prodotto e visualizzare i dati immessi dagli altri utenti. Di tutto ciò ne beneficerà il consumatore finale, che vuole sempre più esser coinvolto riguardo quel che avviene nelle fasi antecedenti l'acquisto del prodotto.

Alcuni player hanno già sperimentato la Blockchain nel settore dell'agrifood: ad esempio, il gigante americano della vendita al dettaglio Walmart ha già eseguito

alcuni test per utilizzare la BC al fine di tracciare ogni singolo passaggio di proprietà che i suoi prodotti subiscono prima di arrivare sugli scaffali del negozio e per garantire maggiore sicurezza ai consumatori lungo tutta la filiera del cibo[192]. Tra le altre, anche Unilever e Nestlé hanno intrapreso la via della Blockchain per tracciare la contaminazione degli alimenti.

4.2.4 Retail

Il settore della vendita al dettaglio costruisce il suo business attorno alla fiducia che il cliente ripone nel sistema di vendita scelto. E se si prova a pensare ad un sistema di vendita che permette di mettere in contatto direttamente acquirente e venditore senza intermediari, diversi sono i benefici che entrambe le parti possono trarre. Start-up come Open Bazaar[193] stanno studiando utility basate su registri distribuiti, in cui cliente e venditore vengono messi in contatto senza oneri di

[192] Fonte: "*Sicurezza nella foodchain con la Blockchain di IBM, Walmart e JD.com*", Mauro Bellini, 2018.

[193] Open Bazaar è nata nel 2014 nella forma di open-source software, scaricabile sul proprio computer o smartphone. In tal modo, gli utenti hanno a loro disposizione una piattaforma di e-commerce, come potrebbe essere eBay, ma decentralizzata in una rete *peer-to-peer*, in cui le persone interagiscono direttamente tra di loro, senza commissioni da pagare agli intermediari come, appunto, eBay. Al momento del lancio della versione 2.0 della piattaforma a fine 2017, il network registrava oltre 40.000 nodi accesi in tutto il globo, anche e soprattutto perché la piattaforma permetteva ai propri clienti di utilizzare come mezzo di scambio diverse criptovalute. Non sono però mancate le critiche e le preoccupazioni di chi vede in questi sistemi un modo più veloce ed efficiente per realizzare scambi illegittimi, ancor più se, come nel caso di Open Bazaar, agli utenti viene garantito l'anonimato. A tal proposito, gli sviluppatori hanno previsto la regolazione interna della piattaforma stessa, cioè basata su un meccanismo di feedback e reputazione dei nodi secondo cui ciascuno può recensire gli altri. Fonte: www.etherevolution.eu.

intermediazione associati. In questi casi la fiducia nel sistema è garantita dal sistema stesso, ossia dalle catene di blocchi che lo costituiscono.

Le principali aree di interesse nel settore del retail afferiscono alla necessità di trasparenza della supply chain, per l'ottenimento di minori rischi di contraffazione e consumatori finali in grado di poter verificare in ogni istante tutte le caratteristiche del prodotto (la provenienza, le specifiche dei materiali, etc.): utilizzando il tracciamento e la certificazione dei meccanismi di autenticità, la Blockchain permette al cliente di comprendere e scoprire la storia di ogni prodotto.

Una recente ricerca[194] di Juniper Research ha rilevato che i ricavi annuali derivanti dalla Blockchain sul tracking delle attività retail saliranno a ben 4,5 miliardi di dollari entro il 2023. Secondo questo studio, infatti, la versatilità della Blockchain riesce a offrire ai rivenditori una trasparenza nella catena di fornitura, nella gestione della fidelizzazione dei clienti e nell'efficienza operativa e, tra gli altri vantaggi, porta anche ad un'adozione più rapida rispetto ad altri settori.

4.2.5 Internet of Things

Un modello di sviluppo che sta velocemente diffondendosi nel tessuto industriale è quello dell'Internet of Things (IoT), ossia l'interconnessione di dispositivi in

[194] Fonte: Juniper Research, 2019.

modo tale che possano scambiare informazioni tra di loro. E una rete di IoT può trovare nella Blockchain la possibilità di identificare in modo rapido e sicuro gli oggetti interconnessi tra di loro, eliminando la necessità di avere delle persone dietro agli oggetti che ne permettano il riconoscimento e attivino quindi lo scambio di informazioni tra essi: la natura decentralizzata e sicura della Blockchain ne fa una tecnologia ideale per la comunicazione tra i singoli nodi di una rete IoT[195].

A tal proposito, l'idea di IBM di fondere l'IoT con la Blockchain ha preso vita nel 2015 tramite il progetto ADEPT (Autonomous Decentralized Peer-to-Peer Telemetry Proof-of-Concept) in collaborazione con Samsung con cui sono stati realizzati *smart contract* su struttura Ethereum. Con ADEPT si è costituita una rete decentrata di dispositivi IoT che poggia su un registro pubblico tramite cui comunicano tra di loro gestendo in modo autonomo la questione del riconoscimento. Il sistema poggia su tre protocolli open source distinti: Telehash per la messaggistica, BitTorrent per il file sharing ed Ethereum per funzioni di coordinamento dei device come per esempio la registrazione, l'autenticazione e la gestione delle regole per l'avvio delle operazioni e per l'autorizzazione di

[195] Una volta adattata agli ambiti applicativi dell'Internet of Things, la Blockchain utilizzerà lo stesso meccanismo in uso nelle transazioni finanziarie che stanno alla base della gestione dei Bitcoin per creare record immutabili associati ai dispositivi intelligenti e agli scambi di dati che avvengono tra questi oggetti smart. Ciò consentirà ai device smart di comunicare direttamente, in totale autonomia, e verificare la validità delle transazioni senza la necessità di un'autorità garante centralizzata. I dispositivi vengono registrati nelle Blockchain una volta entrati all'interno di una rete IoT affinché possano elaborare in autonomia le transazioni. Fonte: "*IoT e Blockchain, il binomio alla base della digital transformation",* Mauro Bellini, 2017.

eventuali transazioni. Grazie all'implementazione di queste soluzioni, per esempio, una lavatrice connessa può diventare un "dispositivo semi-autonomo" in grado di gestire la propria fornitura di materiali di consumo (come detersivo e ammorbidente), l'avvio e lo spegnimento dei programmi, gli interventi di manutenzione, l'ottimizzazione dei cicli di lavaggio per abbattere i consumi energetici, nonché le interazioni con gli altri dispositivi intelligenti della smart home[196].

4.2.6 Sanità

La pandemia da COVID-19 sta mettendo a durissima prova i sistemi sanitari, indipendentemente dal loro grado di sviluppo e dalla relativa ricchezza dei diversi Paesi colpiti. La crisi ha messo a nudo le debolezze dei sistemi sanitari di tutto il mondo, in special modo nel settore dello scambio dei dati su larga scala e dei sistemi di sorveglianza e monitoraggio a livello di popolazione, che sono stati insufficienti a consentire una gestione efficace della pandemia. In un simile contesto, si è molto parlato del potenziale ruolo delle tecnologie digitali nell'affrontare le sfide poste dal COVID-19. In particolare, molte istituzioni pubbliche ed enti privati hanno esplorato con particolare interesse il possibile

[196] Fonte: IBM e Samsung, 2017.

utilizzo della tecnologia Blockchain per lo scambio, la raccolta e la certificazione dei dati.

Considerata la versatilità della Blockchain, non sorprende come siano diversi gli scenari ipotizzati per il suo utilizzo: si passa dalla certificazione delle identità alla certificazione dei tamponi, dal contact tracing alla certificazione dell'affidabilità delle notizie relative alla pandemia, dal controllo delle quarantene al tracciamento dei kit per i test, fino alla gestione trasparente degli aiuti economici pubblici e privati[197]. Altro importante elemento è lo scambio di dati fra Paesi, che facilita la connessione fra database altrimenti isolati gli uni dagli altri, e dunque non pienamente utilizzabili per gestire la pandemia[198]. L'uso della tecnologia può inoltre facilitare il coinvolgimento dei cittadini, offrendo loro strumenti trasparenti per la condivisione dei dati personali e maggiore controllo su di essi, incoraggiando la collaborazione collettiva per lo scambio di dati volto al controllo della pandemia[199].

Con la disponibilità dei vaccini (si pensi a quelli annunciati da Pfizer e Moderna), altre applicazioni riguardano il tracciamento della supply chain dei vaccini stessi, oltre che dei già citati kit e reagenti per i test. Nel caso dei primi il potenziale utilizzo si fa più interessante, laddove i vaccini hanno (stando alle dichiarazioni

[197] Fonte: "*Il ruolo della tecnologia blockchain per combattere la pandemia da COVID-19*", Mirko De Maldè, 2020.
[198] Fonte: "*Il ruolo della tecnologia blockchain per combattere la pandemia da COVID-19*", Mirko De Maldè, 2020.
[199] Fonte: "*Il ruolo della tecnologia blockchain per combattere la pandemia da COVID-19*", Mirko De Maldè, 2020.

delle case produttrici) una vita media fra i cinque e i trenta giorni a temperature che non superino gli 8 gradi: la certificazione delle corrette condizioni di trasporto e conservazione, in combinazione con appropriati dispositivi IoT, sembra essere una prospettiva interessante per l'impiego della tecnologia Blockchain.

Quanto al tracciamento dei test, l'uso della tecnologia appare interessante per certificare origine e distribuzione dei test e dei reagenti, ma anche per certificare i risultati, il luogo e la data dove un certo test è stato svolto, soprattutto per mappare le aree più a rischio di diventare focolaio.

Un altro ruolo importante può essere svolto dalla Blockchain nel contrasto alla disinformazione dilagante, che vede nella pandemia uno dei settori più prolifici: i flussi informativi riguardo la pandemia sono sicuramente stati oggetto di inquinamento da parte di fonti poco attendibili e faziose[200]. Per arginare questo fenomeno, la tecnologia Blockchain può essere d'aiuto, grazie alle sue caratteristiche chiave di distribuzione e condivisione, per certificare e garantire la provenienza e l'affidabilità delle informazioni, anche tramite il mantenimento di un unico corpo informativo sempre aggiornato e sincronizzato fra le diverse fonti accreditate, facilitando così la diffusione di informazioni corrette e marginalizzando le informazioni isolate e le fake news.

[200] Fonte: Khurshid, A. (2020). "Applying blockchain technology to address the crisis of trust during the COVID-19 pandemic". JMIR medical informatics.

L’associazione internazionale INATBA (International Association of Trusted Blockchain Applications) ha come compito istituzionale quello di supportare l’adozione mainstream delle Distributed Ledger Technology in diversi settori, coinvolgendo imprese, decisori pubblici, organizzazioni internazionali, enti regolatori e la società civile. Considerata questa missione e la sua dimensione internazionale, all’esplodere della pandemia da COVID-19, INATBA ha lanciato una serie di iniziative per il rallentamento della pandemia e la gestione della crisi nei vari settori dell’economia e della società. Nello specifico, ha strutturato la propria iniziativa tramite il lancio di una Task Force COVID, una rete globale di enti pubblici e privati impegnati a rendere operative soluzioni basate su Blockchain per supportare le istituzioni pubbliche nell’affrontare l’emergenza. La Task Force è strutturata attorno al coinvolgimento di tre fondamentali categorie di stakeholder: enti pubblici, industria, istituzioni accademiche. In particolare, INATBA ha ottenuto l’immediato coinvolgimento diretto della Commissione Europea e dell’University College di Londra (UCL).

Varie proposte sono state presentate nel corso della prima fase di analisi, coprendo una ampia gamma di scenari, da sistemi di identità digitale, a sistemi per la verifica dei test, fino alla gestione facilitata dei trial clinici, passando per sistemi di tracciabilità della supply chain farmacologica, specialmente per

combattere il fenomeno della contraffazione[201]. Interessanti erano anche le diverse proposte presentate per consentire una più efficiente gestione dei fondi pubblici destinati a supportare cittadini e imprese in questa fase di contrazione economica, così da evitare abusi e facilitare la tracciabilità degli aiuti. Similmente, sono stati presentati sistemi per facilitare società private nel reperimento di sostegni, dimostrando ancora più chiaramente il grande potenziale delle Distributed Ledger Technology nel supportare la battaglia contro il COVID-19.

4.2.7 Pubblica Amministrazione

La Blockchain nella Pubblica Amministrazione trova utili ed evidenti ambiti applicativi, soprattutto se si considera che grazie a questa tecnologia ogni cittadino potrebbe veder creata una propria identità digitale, condivisa e implementata in questo sistema, con diversi vantaggi, tra cui: rendere più difficile l'evasione fiscale, avere un controllo maggiore dei cittadini e quindi combattere la criminalità, creare servizi semplificati in tutti i settori della PA (ad esempio, l'invio di dati semplificato), e molto altro[202]. PA e sistema welfare sono i settori nei quali le tecnologie Blockchain possono contribuire a semplificare le lunghe procedure burocratiche per ottenere, ad esempio, l'erogazione di aiuti pubblici

[201] Fonte: "*Il ruolo della tecnologia blockchain per combattere la pandemia da COVID-19*", Mirko De Maldè, 2020.
[202] Fonte: "*Blockchain per Risk Management e Governance nell'e-voting*", *Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia,* Mauro Bellini, 2020.

solamente nelle situazioni in cui effettivamente sussistono le condizioni stabilite per legge, riducendo fenomeni di truffe. Tramite lo sviluppo di registri distribuiti, la PA potrebbe mantenere sotto controllo alcune specifiche situazioni di norma difficilmente gestibili. Si pensi, per ipotesi, al mercato della compravendita di armi[203]: tramite BC si potrebbero sviluppare registri pubblici più sicuri in cui ai candidati non ritenuti idonei viene impedito l'acquisto di armi o l'ottenimento di un porto d'armi. Un passo successivo potrebbe essere quello di collegare a questi registri le cartelle cliniche di tutti gli individui, rendendo quindi molto più veloce per le forze dell'ordine la ricerca di soggetti con profilo psicologico debole che potrebbero essere più inclini alla violenza.

Una delle concrete applicazioni senz'atro più interessanti nell'ambito pubblico riguarda l'uso di strutture Blockchain per rendere più sicuro l'e-voting[204]. Il voto elettronico è da lungo tempo oggetto di sperimentazioni ma resta da sempre irrisolto il tema della sicurezza. Numerose le minacce e i rischi collegati al voto elettronico, che possono essere codificate in quattro punti[205]:

1. Manipolazione dell'opinione pubblica con azioni volte a influenzare le tendenze;

[203] La startup americana Blocksafe, a questo proposito, sta costruendo un network Blockchain per la condivisione e il mantenimento di dati IoT: in particolare permette di tenere traccia della posizione della propria arma nel mondo, limitando il numero di casi di violenze che hanno come punto di partenza il furto di un'arma. Fonte: www.blocksafetech.com.
[204] Fonte: Blockchain per Risk Management e Governance nell'e-voting, "*Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia*", Mauro Bellini, 2020.
[205] Fonte: Blockchain per Risk Management e Governance nell'e-voting, "*Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia*", Mauro Bellini, 2020.

2. Violazione delle identità;
3. Intrusioni nei sistemi e manipolazione dei dati;
4. Azioni di sabotaggio sulle azioni di voto.

E come hanno dimostrato le esperienze di diversi Paesi, la risposta circa il tema della sicurezza può venire dalla Blockchain: gli Asset Digitali Unici rappresentano una delle basi che permettono alla Blockchain di portare nuove forme di garanzia nel voto elettronico.

Secondo la società CB Insight, che ha clusterizzato i vari passaggi che si susseguono in caso di e-voting, il Digital Voting Journey presenterebbe dei pericoli già nella fase precedente alla votazione (fase *pre-election*), momento in cui il cittadino viene "bombardato" di notizie appositamente alterate per influenzare la sua opinione. Successivamente (fase *election*), operazioni di *hacking* possono modificare l'effettiva scelta di un individuo generando, in ultima istanza (fase *post-election*), dispute post-elettorali[206]. Introducendo un approccio basato sulla Blockchain si può giungere ai seguenti miglioramenti[207]:

– Prima delle elezioni (*pre-election*) i rischi di influenza mediatica possono essere ridotti tramite appositi strumenti crittografici che "filtrano" le notizie provenienti da diverse fonti, gestendo la quantità e la qualità delle informazioni che ogni utente può ricevere;

[206] Fonte: "*How Blockchain Could Secure Elections*", www.cbinsights.com.
[207] Fonte: "*How Blockchain Could Secure Elections*", www.cbinsights.com.

- Durante la fase di voto vera e propria (*election*) viene verificata l'identità dell'elettore e l'unicità del suo voto;
- A seguito della votazione (*post-election*) è possibile effettuare degli audit per il conteggio dei voti garantendo trasparenza e immutabilità delle scelte effettuate dai cittadini.

Follow My Vote è un'applicazione per l'e-voting sviluppata in America basata sulla tecnologia Blockchain che permette ai suoi utenti di accedere, direttamente dall'applicazione installabile su smartphone, ad un'area privata in cui essi possono autenticarsi grazie alla webcam e successivamente votare e seguire in tempo reale i risultati delle elezioni, senza la minaccia di vedere alterato il proprio voto[208]. Sempre negli U.S.A., c'è anche Blockchain Technologies Corp., con sede a New York, che sta adottando un approccio ibrido di sistema di voto azionato da Blockchain abbinato a schede cartacee che utilizzano codici QR per garantire che ogni voto venga assegnato una sola volta[209]. Stiamo assistendo a un maggiore movimento nella direzione del voto basato su Blockchain anche al di fuori degli Stati Uniti: il servizio di posta australiana di proprietà del governo, ad esempio, utilizza la tecnologia BC per creare un sistema di votazione agnostico, a prova di manomissione, rintracciabile e anonimo, che si dimostrerebbe resistente agli

[208] Fonte: "*E-Voting e blockchain, sì o no: i casi internazionali*", Eloisa Marchesoni, 2017.
[209] Fonte: Marchesoni, 2017.

attacchi di tipo Denial of Service (DoS)[210]. Anche il depositario centrale di titoli della Russia, l'NSD, ha applicato la Blockchain all'e-voting, progettando un sistema di voto e-proxy, un libro mastro sul quale vengono trasmesse e conteggiate le azioni di voto[211]. Un altro Paese che cerca di sfruttare la tecnologia Blockchain per il voto è l'Estonia[212], che è già leader nell'applicazione alla politica della tecnologia, con il suo programma di e-residency, una piattaforma di identità elettronica che consente agli stranieri di accedere ai servizi governativi. Il paese sta completando gli sforzi precedenti con un sistema di voto elettronico basato su Blockchain che consente sia ai cittadini estoni che agli e-residenti di votare in modo sicuro nelle assemblee degli azionisti delle società estoni. Sistemi di voto su Blockchain stanno facendo il loro debutto anche in Medio Oriente, presso la Borsa di Abu Dhabi[213], che l'anno scorso ha annunciato di aver iniziato ad utilizzare Blockchain per consentire alle parti interessate di partecipare e osservare i voti nelle loro riunioni annuali generali.

4.2.8 Mondo accademico

Nell'ambito accademico, nonostante la digitalizzazione abbia reso più immediate molte delle procedure attuali, i controlli manuali e le attività burocratiche sono

[210] Fonte: Marchesoni, 2017.
[211] Fonte: Marchesoni, 2017.
[212] Fonte: Marchesoni, 2017.
[213] Fonte: Marchesoni, 2017.

ancora le più time consuming. Inoltre, la contraffazione di certificati è una delle frodi più frequenti ai danni di numerosi studenti e docenti. Secondo varie ricerche pubblicate dalla BBC nel 2018, gli Stati Uniti sono al centro del mercato legato a università false e diplomi di laurea contraffatti con circa 800 istituti già identificati come fasulli e molti altri sotto inchiesta[214].

Pertanto, diversi istituiti tentano già di limitare il fenomeno con contromisure di vario tipo: dal divieto di pubblicare foto con il proprio diploma sui social, ai certificati con QR code, fino all'innovativo programma avviato dal prestigioso Massachussets Institute of Technology (MIT) americano e ripreso poi da alcuni atenei di tutto il mondo, tra cui l'università di Cagliari, prima in Italia nel 2018. Per la prima volta, infatti, l'ateneo sardo ha utilizzato la tecnologia Blockchain per autenticare i certificati di Laurea della facoltà di informatica tramite il sistema fornito dalla piattaforma Ethereum[215]. Detto certificato viene elaborato proprio come uno *smart contract*, che si attiva in maniera automatica al raggiungimento di condizioni prestabilite dagli utilizzatori.

Sempre in questo ambito, Cineca, in collaborazione con l'Università Milano Bicocca, ha sviluppato un nuovo sistema di certificazione basato su Blockchain

[214] Fonte: BBC, 2018.

[215] "*Abbiamo deciso di garantire l'autenticità dei certificati europei dei nostri laureati con questa tecnologia, perché intendiamo dotarli di uno strumento moderno, semplice e immediato, utilizzabile ovunque nel mondo. Un certificato di laurea, sia cartaceo che in formato digitale, è facilmente falsificabile o alterabile. Grazie a questa tecnologia, i nostri studenti potranno garantire l'autenticità e l'integrità dei loro certificati digitali a potenziali datori di lavoro in tutto il mondo, in modo semplice e gratuito*". Fonte: "*Certificati di laurea, autenticità garantita con la Blockchain*", Università degli Studi di Cagliari, 2018.

per garantire l'autenticità del titolo di Laurea. Esso garantisce la notarizzazione dei titoli di studio introducendo lo standard Blockcerts sviluppato dal MIT[216]: in questo modo il titolo sarà verificabile in tempo reale sul web, senza passare attraverso le richieste agli atenei e le trafile burocratiche.

Inoltre, c'è chi ha inteso i benefici derivanti dalla decentralizzazione forniti dalla Blockchain e ha così immaginato un tipo differente di università, maggiormente distribuita e democratica. L'idea ha portato, nel 2018, alla nascita della Woolf University, intendibile come una piattaforma in cui gli studenti ricevono ugualmente gli insegnamenti dai docenti e superano gli esami al fine di conseguire il titolo finale[217]. Ciò al fine di voler eliminare l'intermediario "università", inteso come sistema burocratico, fatto di procedure e rigide tempistiche da rispettare. La piattaforma permette inoltre una gestione dei dati più sicura ed efficiente, tramite l'utilizzo di un sistema che automatizza le procedure amministrative. Chiavi di check-in (per esempio, un pulsante da premere sul proprio smartphone) per studenti e docenti attivano *smart contract* validando la partecipazione dello studente ad una lezione o esame. E data la trasparenza del registro pubblico, chiunque e in qualsiasi momento potrà controllare le informazioni contenute nella Blockchain di Woolf[218].

---

[216] Fonte: "*Bicocca rilascia le prime certificazioni di laurea Blockcerts*", Università degli Studi di Milano Bicocca, 2019.
[217] Fonte: "*Building the first Blockchain University*", Dr. Joshua David Broggi *et al*., 2018.
[218] Fonte: Dr. Joshua David Broggi *et al*., 2018.

4.2.9 Sport

Quello dello sport potrebbe diventare un nuovo bacino di investimento per le tecnologie Decentralized Ledger.

L'americana FCFL, Fan Controlled Football League[219], per prima, ha avviato un esperimento che mira a reinventare il rapporto tra tifosi e sport, fornendo ai primi il pieno controllo della propria esperienza da spettatori tramite la produzione dei cosiddetti Fan Token. Questi Token rappresentano il controllo che ciascuno spettatore ha sulla FCLF: più un fan guarda le partite o dà prova del suo interesse, più Token acquisisce e più decisioni può prendere, dalla scelta del coach secondo lui più idoneo alla tattica da mettere in piedi durante il gioco. Si tratta di una vera e propria "democratizzazione" dello sport[220].

Il principale ambito di applicazione della presente tecnologia sullo sport riguarda senz'altro il Management delle società sportive: la gestione delle azioni e delle decisioni societarie, ad esempio, passerà attraverso piattaforme decentralizzate che permettono la vendita di azioni e diritti ai fan sparsi nel mondo in maniera rapida e sicura[221].

[219] Si tratta della prima lega professionistica sportiva ad essere stata disegnata secondo i meccanismi della Blockchain, grazie alla quale i tifosi possono entrare in pieno controllo della propria esperienza di intrattenimento, assumendo giocatori, scegliendo di assumere/licenziare gli allenatori, chiamando gli schemi e tanto altro. Fonte: "*Come integrare la Blockchain nel mondo dello* sport", Giancarlo Diamanti, 2018.

[220] Fonte: Diamanti, 2018.

[221] Fonte: SportsTechX, 2018.

La Blockchain è in grado di impattare altresì sulla Performance sportiva degli atleti[222]: in questo ambito si trovano le interessanti proposte di Lympo (*cap. 3*, *par. 3.3.2*), che propone una rivoluzione dell'intero ecosistema dell'healthy lifestyle, creando un sistema di ricompense, attraverso *smart contract*, a seguito dei dati generati da ogni utente nello svolgimento delle loro performance fisiche. Per intenderci, ogni utente può decidere di partecipare ad una sfida (per esempio una corsa di 5 km): tramite tecnologia Blockchain, viene sottoscritto un contatto con il soggetto promotore e, al termine della corsa, Lympo scaricherà i dati del tracking confermando il completamento della sfida. L'utente potrà quindi ricevere la sua ricompensa in forma di LYM Token.

Un altro ambito sportivo nel quale la tecnologia può trovare utili ambiti applicativi è quello Media&Fan, puntando ad arricchire il fan engagement[223]: la *tokenizzazione* del fan system permetterà l'accesso a contenuti e servizi esclusivi, investendo e guadagnando dal successo del proprio atleta preferito.

Infine, la Blockchain potrebbe risultare lo strumento definitivo per eliminare il fenomeno della falsificazione dei biglietti in occasione degli eventi sportivi, garantendo anche una maggiore sicurezza all'interno degli impianti[224].

[222] Fonte: SportsTechX, 2018.
[223] Fonte: SportsTechX, 2018.
[224] Fonte: "*Cosa succede quando blockchain e sport industry si incontrano*", Emanuela Perinetti, 2018.

4.2.10 Car sharing

Nell'ambito del car sharing la presente tecnologia si pone al servizio di quelle applicazioni che intendono proporsi come "anti-centralizzate". Si tratta di sostituire la comune rete centralizzata utilizzata per chiamare i taxi, con alcune applicazioni che i clienti possono utilizzare per cercare altri individui che viaggiano su percorsi simili, servendosi di criptomonete per pagare il passaggio[225].

Molte società sono già attive in Italia nel "car sharing *peer-to-peer*". Parliamo, per esempio, della bolognese Auting, azienda con cinquemila utenti e più di mille vetture in strada, e della milanese Genial Move, operativa dall'autunno 2017: il loro servizio permette e facilita la condivisione di un veicolo non utilizzato dal proprietario con persone iscritte ad una specifica piattaforma per la registrazione e il pagamento del servizio.

Da dicembre 2018 è operativo in Italia il servizio offerto da Helbiz, start-up statunitense, che si rivolge direttamente ad ogni singolo automobilista o possessore di scooter che intende dare in noleggio il proprio mezzo per un breve lasso di tempo. L'obiettivo della società è quello di creare una comunità di persone che condividono il proprio mezzo con tutti gli iscritti. Helbiz sfrutta la tecnologia Blockchain: a differenza degli attuali e suddetti car-sharing *peer-to-*

[225] Fonte: "*Car sharing peer-to-peer: un'analisi empirica sulla città di Milano*", Mariotti Ilaria, Beria Paolo, Laurino Antonio, Università degli Studi di Trieste, 2013.

peer, che prevendono procedure tra cui lo scambio manuale delle chiavi o la sottoscrizione di contratti di condivisione, la start-up americana punta tutto sugli smartphone e sul loro collegamento con una sorta di scatola nera legata alla centralina dell'auto. Infatti, basta iscriversi, tramite apposita app, al servizio offerto da Helbiz, per ottenere la chiave digitale necessaria a mettere in moto il veicolo. Successivamente è la scatola, fornita in modo gratuito agli utilizzatori, a controllare tutto, dal funzionamento dell'auto ai chilometri percorsi fino a eventuali incidenti o necessità di soccorso. È sempre la scatola ad inviare poi i dati necessari per gli addebiti all'utilizzatore.

Inoltre, l'industria dei trasporti ha iniziato a muovere i primi passi a livello mondiale con la creazione del consorzio MOBI, acronimo di Mobility Open Blockchain Initiative, per coordinare e promuovere iniziative relative all'utilizzo della Blockchain nella mobilità[226]. La mission del consorzio è quella di definire linee guida sullo sviluppo della mobilità intelligente, tra cui la digital identity dei veicoli, le modalità di condivisione dei driving data, la gestione delle transazioni legate al car-sharing. Il consorzio si fa inoltre promotore della MOBI Grand Challenge 2018/2019, con l'obiettivo di alimentare la rivoluzione dei veicoli a guida autonoma, studiando nello specifico, il modo in cui questi veicoli inviano e ricevono dati e coordinano i propri movimenti tramite la Blockchain. A tal

[226] Fonte: "*Mobi, il consorzio nato per studiare come la blockchain rivoluzionerà l'industria dell'auto",* Franco Velcich, 2018.

proposito, MOBI vede la partecipazione di diversi operatori attivi nel mondo dei trasporti, dalle grandi case automobilistiche come Ford, General Motors, Renault e Bmw, ad aziende di componentistica come Bosch e ZF Friedrichshafen, a società di consulenza come Accenture e informatiche come IBM, a dimostrazione di un'iniziativa volta a creare un vero e proprio ecosistema per lo sviluppo delle innovazioni digitali volte a rendere la mobilità sempre più intelligente.

4.3 Riflessioni di sintesi

A conclusione della overview sulle attuali e potenziali applicazioni della presente Tecnologia, è opportuno sottolineare che, nel prossimo futuro, potrebbero essere inglobati nell'universo Blockchain tutti quegli ambiti in cui le potenzialità di una struttura che è in grado di garantire la validità di una transazione registrata in un database sicuro e distribuito permettono notevoli vantaggi rispetto al tradizionale sistema centralizzato.

L'identificazione degli attuali impatti economico-aziendali della Blockchain esaminati nel corso della trattazione, infatti, permette di far emergere il contesto operativo e competitivo nel quale le aziende si troveranno ad operare nel prossimo futuro. Da attività quasi hobbystica e alla portata di chiunque disponesse di un personal computer, il sistema è diventato nel tempo una vera e propria industria

professionistica e capital-intensive: nell'industry delle criptovalute lavorano più di 2.000 addetti e qualche centinaio di aziende tra "Exchange" (le piattaforme dedicate all'acquisto, alla vendita e al trading delle criptovalute), "Wallets" (dove le criptovalute vengono conservate), "Miners" (coloro che assicurano la correttezza delle transazioni registrate sulla blockchain) e "Payments" (aziende che facilitano l'uso delle criptovalute quale mezzo di acquisto e transazione). Si tratta di una industry nata dall'esigenza di affiancare gli utenti meno esperti nella gestione dei propri wallet e delle transazioni, ma anche per favorire la convertibilità di Bitcoin e delle altre criptovalute in valuta nazionale corrente. Una industry che, a differenza di quanto recita la narrativa di Bitcoin, cerca continuamente il confronto con le istituzioni finanziarie nazionali. Infatti, più della metà degli Exchange nord-americani ed europei e un quarto dei Wallet provider vanta una licenza rilasciata da un ente regolatore, e più dell'80% delle aziende che effettuano servizi di Payments dichiara di aver stipulato accordi con banche e network di pagamenti.

Questo nuovo sistema, tuttavia, non è privo di effetti indesiderati, innanzitutto per quanto riguarda l'ambiente: il consumo di energia elettrica per il solo Bitcoin è pari a 10.41 terawattora annui, pari al consumo di energia di un Paese di 3,3 milioni di abitanti. Minacciati dagli effetti perversi della speculazione, dal dimezzamento del premio previsto dal protocollo, dalla crescita del costo dell'energia, da una competizione sempre più sofisticata e dalla necessità di un

continuo afflusso di capitali per poter mantenere l'apparecchiatura all'altezza del fabbisogno, i Miners stanno incrementando la loro dipendenza dai costi di commissione[227]. Inoltre, quasi il 70% dei bitcoin attualmente in circolazione è posseduto da meno dell'1% dei wallet. Questa concentrazione è "ingiustificabile" dal punto di vista della quantità di lavoro effettivo svolto dai Miners, che li rende detentori di un "potere di pressione" che potrebbe avere conseguenze molto gravi nell'eventualità che bitcoin possa sostituirsi, in tutto o in parte, alle monete nazionali[228]. In aggiunta, è pur vero che le criptovalute possono essere accettate e facilmente scambiate in tutto il mondo, non avendo bisogno di alcun supporto fisico né di un intermediario che ne verifichi l'attendibilità, ma l'alta volatilità del loro valore, e quindi del loro potere d'acquisto, le rende un mezzo di pagamento non affidabile, limitandone per ora l'accettabilità[229]. "*L'economia a cui Bitcoin rinvia è un'economia in cui nessuna relazione che non sia istantanea può essere contemplata. La società peer-to-peer implicata da Bitcoin è una società individualistica, basata sul principio della inviolabilità dei contratti. È questa la conseguenza necessaria del ripudio incondizionato nella fiducia di un terzo. Nulla può intervenire per modificare ciò che è stato deciso contrattualmente dalle*

[227] Fonte: Tapscott, D., Tapscott, A., "*The Impact of the Blockchain Goes Beyond Financial Services*", Harvard Business Review, 2016.
[228] Fonte: Amato, M., Fantacci, L., "*Per un pugno di bitcoin: rischi e opportunità delle monete virtuali",* Università Bocconi Editore, 2016.
[229] Fonte: Amato, M., Fantacci, L., "*Per un pugno di bitcoin: rischi e opportunità delle monete virtuali",* Università Bocconi Editore, 2016.

parti"[230], con il paradosso che nemmeno le parti possono intervenire per trovare un compromesso accettabile (ad esempio nel caso di un debito non saldato per tempo a causa di sopraggiunte difficoltà economiche del debitore). È intuibile, pertanto, che nella cripto-economia il posto della legge sia preso dal codice informatico: la fede politica di Bitcoin è riposta proprio nel fatto che sia possibile una ricreazione informatica del mondo economico. Inoltre, "*a livello di ambizioni dichiarate, il Bitcoin è la moneta dell'economia globalizzata, nel senso preciso di un'economia caratterizzata dall'assenza di confini e dalla messa in scacco dei poteri di controllo*"[231]. Non è un caso, infatti, che i Bitcoin siano sempre più utilizzati nell'acquisto di prodotti illegali: finché potranno continuare a essere usati impunemente e senza possibilità di controllo per attività nocive agli interessi della collettività, non potranno guadagnarsi la fiducia della maggior parte delle imprese e delle persone comuni.

Alla luce di queste informazioni, molte delle premesse che hanno accompagnato il successo mediatico della Blockchain e delle criptovalute in questi anni (come la disintermediazione delle istituzioni finanziarie, l'azzeramento dei costi, il sostegno all'e-commerce e al commercio globale, il ritorno del controllo dell'individuo sulle proprie finanze) sembrano essere ben lontane dal realizzarsi.

---

[230] Fonte: Amato, M., Fantacci, L., "*Per un pugno di bitcoin: rischi e opportunità delle monete virtuali",* Università Bocconi Editore, 2016.

[231] Fonte: Amato, M., Fantacci, L., "*Per un pugno di bitcoin: rischi e opportunità delle monete virtuali",* Università Bocconi Editore, 2016.

E se gli impatti della Blockchain a livello di business risultano per molti versi ancora incerti, a livello di società appaiono tutti da scoprire. Oggi è forse troppo presto per capire o prevedere l'impatto potenziale della Blockchain sulla nostra società: ne abbiamo sentore ma non ancora una vera esperienza diffusa, con l'unica eccezione, peraltro controversa, dei Bitcoin.

Le "note di banco", da cui le moderne banconote o cartamonete, sono la più importante innovazione tecno-finanziaria del XIV secolo. Essa ha contribuito in maniera rilevante allo sviluppo economico, rendendo più sicuri gli scambi commerciali, e quindi culturali del tempo, dando vita al Rinascimento. I Bitcoin, e prima ancora la Blockchain, potrebbero essere la più importante innovazione tecno-finanziaria del XXI secolo e contribuire in maniera altrettanto rilevante allo sviluppo economico, rendendo più sicuri gli scambi commerciali, e quindi culturali di oggi, dando vita a un nuovo Rinascimento[232].

Volendo approfondire i potenziali impatti sociali della Blockchain, le categorie poste agli estremi del continuum tracciato da Umberto Eco ("Apocalittici e integrati"[233]) appaiono ancora valide. Il dibattito circa gli impatti socio-culturali della Blockchain sembra infatti non poter sfuggire alle due fazioni opposte: i primi preoccupati, a diverso titolo, dell'effetto di questa tecnologia sulle relazioni umane; i secondi convinti che gli algoritmi che la governano siano la chiave per

[232] Fonte: Ferrari, R., 2016, "*L'Era del Fintech*", Franco Angeli.
[233] Fonte: Umberto Eco, 1964.

un nuovo umanesimo digitale. La Tecnologia, come sappiamo, si basa sull'utilizzo di sofisticati algoritmi che si propongono come dei nuovi sistemi esperti in grado di sostituire (apocalittici) o migliorare (integrati) le capacità umane[234]. Di fatti, la Blockchain agisce su due colonne portanti del fare società: la conoscenza e la fiducia condivisa (*cap. 3, fig. 26*). In tal senso, partendo dai campi in cui gli impatti attesi della Tecnologia sono più profondi, è da chiedersi quali siano i percorsi di regolazione e le azioni di governance capaci di valorizzarne i potenziali benefici per la società, riducendone i presumibili rischi. Ripercorrendo il contrasto tra apocalittici e integrati, è possibile trovare una risposta a tale quesito. Da un lato, è vero che la società automatica che tanto preoccupa Bernard Stiegler è qualcosa di più di un opaco scenario[235]: cittadini e consumatori sono sempre più "pigri" e delegano ad algoritmi ben studiati le loro capacità di scelta nei più disparati campi del vivere comune, dalla musica al consumo, passando addirittura per le relazioni sentimentali. È innegabile, infatti, che una parte delle conoscenze veicolate, in generale, dagli strumenti di Intelligenza Artificiale non abbia stimolato un aumento dello stato di apprendimento ma che, come in un principio entropico, tali conoscenze siano state trasferite dall'uomo alla macchina. Un discorso simile lo si può fare per la Blockchain, data la sua capacità di sostituire con un algoritmo la fiducia che le persone nutrono verso talune

[234] Fonte: Anthony Giddens, "*Le conseguenze della modernità. Fiducia e rischio, sicurezza e pericolo",* 1994.
[235] Fonte: Bernard Stiegler, 2019.

organizzazioni (Stati, banche centrali, categorie professionali, ecc.). Tutt'altro che apocalittiche, rispetto alle nuove tecnologie, sono le opinioni di altri pensatori come Michael Shellenberger, che vedono nel progresso tecnologico l'unica speranza per salvarci da un'apocalisse ambientale[236]: in tal senso, le innovazioni tecnologiche diventerebbero degli strumenti necessari per governare la complessità che ci circonda. In particolare, la Blockchain migliorerebbe la tracciabilità alimentare, la gestione dei rifiuti o l'efficientamento del mercato dell'energia.

Tali contrapposizioni ideologiche identificano come i possibili sviluppi futuri della Tecnologia e i suoi impatti sulla società siano ancora sfocati nei loro contenuti. Ci troviamo, dunque, di fronte ad un futuro tutto da scrivere, ricco certamente di potenzialità ma con molte incognite ancora da risolvere.

[236] Fonte: Michael Shellenberger, 2020.

CONCLUSIONI

A seguito di una breve disamina dei principali concetti teorici alla base della struttura di una Blockchain, la prima parte della trattazione descrive dettagliatamente le modalità di funzionamento della stessa. Solo dopo aver compreso la fisionomia e l'anatomia della Tecnologia, infatti, è possibile coglierne appieno i benefici in ambito economico-aziendale. La Tesi delinea, pertanto, le principali applicazioni della Blockchain, soffermandosi in particolare sulla descrizione degli *smart contracts*, strumenti in grado di rivoluzionare la contrattualistica tradizionale e, se vogliamo, il modo di fare business. La trattazione prosegue poi analizzando i progetti sviluppati da aziende italiane ed estere, con l'obiettivo di sottolineare le applicazioni della Tecnologia nei vari settori dell'economia: dall'ambito Finance a quello dell'Agrifood e del Retail, da quello della Pubblica Amministrazione allo sport, passando per il settore sanitario e accademico. In questa sede emerge, tuttavia, come il numero di progetti sin ora avviati sia molto esiguo, ancor più se si considerano solamente quei casi in cui l'adozione della Blockchain ha raggiunto livelli di analisi e progettazione sufficienti da poterla descrivere in termini di benefici e costi rilevati o stimati. Ciò nonostante, si è potuto rilevare, per i casi considerati, un vivo interesse da parte

degli attori coinvolti per la condivisione e il confronto dei risultati raggiunti, a testimonianza di un clima generale di entusiasmo e cooperazione.

Non possiamo però sfuggire dal considerare i principali punti di debolezza della Tecnologia e del cambiamento che essa sta generando. Primi fra tutti, limiti strettamente tecnologici che riguardano aspetti come la sicurezza, l'inviolabilità e la scalabilità della struttura. In secondo luogo, la gestione delle interazioni tra gli attori lungo le filiere e il loro coinvolgimento possono rappresentare barriere molto robuste, soprattutto se non tutti percepiscono gli aspetti win-win del sistema. Inoltre, è possibile evidenziare potenziali limiti socio-culturali, dettati dal recepimento della Tecnologia da parte della sfera sociale: come si è verificato con Internet, quando si sviluppa una nuova tecnologia, attorno ad essa si creano vari opinioni che possono essere sia negative che positive. Solo il tempo potrà dire se tale tecnologia è utile o meno e se, soprattutto, sarà in grado di sopravvivere ed essere recepita positivamente. L'unica cosa certa è che "*il clima che si respira attorno alla Blockchain è simile a quello che toccò al Tcp-Ip, il protocollo alla base di internet, nato nell'82*"[237].

Ad oggi non è ben chiaro se la Tecnologia in sé possa introdurre un cambiamento sostanziale nel modo in cui i processi economico-aziendali sono impostati ed organizzati. Nei limiti di questo perimetro di ricerca sembra non trattarsi, almeno per ora, di un nuovo approccio disruptive in tal senso. Ciò che invece è

[237] Fonte: SOLE24ORE, Pierangelo Soldavini, 2018.

confermato dai risultatati è l'indubitabile vantaggio prodotto nell'efficientamento delle attività, soprattutto a livello di rapidità nella risoluzione dei blocchi e delle controversie.

In conclusione, la rischiosità della Blockchain non permette oggi alle aziende un livello di confidenza tale da potersi affidare completamente ad essa, motivo per cui viene maggiormente utilizzata come strumento di supporto a livello operativo piuttosto che strategico. Se però questo aspetto verrà in futuro risolto, in uno scenario probabilistico il modo di gestire i singoli business potrà essere fortemente impattato da una logica di decentralizzazione e l'iniziale propensione verso un registro di tipo *permissioned* potrebbe essere solo una fase di transizione verso una logica *public* in cui l'accesso alle informazioni da parte di un qualsiasi nodo del network può attivare transazioni e certificare passaggi di mano senza la necessità di un'azione manuale.

BIBLIOGRAFIA

- Acta Fintech, “Blockchain Banking”, 2020.
- Alharby Maher, Van Moorsel Aad, “Blockchain-based smart contracts: A systematic mapping study”, 2017.
- Alù Angelo, “Blockchain, le principali normative nazionali al mondo”, 2019.
- Amato M., “L’enigma della moneta e l’inizio dell’economia”, Feltrinelli, 2010.
- Amato M., Fantacci L., “Per un pugno di bitcoin: rischi e opportunità delle monete virtuali”, Università Bocconi Editore, 2016.
- Anderson James C., Håkansson Håkan, Johanson Jan, “Dyadic Business Relationships within a Business Network Context”, Journal of Marketing, 1994.
- Arrigo Francesca, “Blockchain e smart contract: funzionamento e applicazioni”, 2019.
- Astley W. Graham, Fombrun Charles J., “Collective Strategy: Social Ecology of Organizational Environments”, 1983.
- Back A., “HashCash”, 2002.

- Bagnoli, Bravin, Massaro, Vignotto, “BusinessModel4.0 - I Modelli di Business vincenti per le imprese italiane nella quarta rivoluzione industriale”, Edizioni Ca’ Foscari, Venezia, 2018.
- Bandiera Barbara, “L’influenza dell’innovazione tecnologica in ambito finanziario”, 2018.
- Bellini Mauro, “Blockchain e Governance: gli ambiti applicativi nell’Impresa 4.0 con le DLT”, 2018.
- Bellini Mauro, “Blockchain per Risk Management e Governance nell’e-voting”, 2020.
- Bellini Mauro, “Blockchain: cos’è, come funziona e gli ambiti applicativi in Italia”, 2020.
- Bellini Mauro, “Blockchain: i benefici concreti e le applicazioni più promettenti per 27 settori”, 2019.
- Bellini Mauro, “IoT e Blockchain, il binomio alla base della digital transformation”, 2017.
- Bellini Mauro, “La roadmap verso i capital market del futuro secondo la Swiss Blockchain Federation”, 2020.
- Bellini Mauro, “Sicurezza nella foodchain con la Blockchain di IBM, Walmart e JD.com”, 2018.
- Bellini Mauro, “Smart Contracts: che cosa sono, come funzionano quali sono gli ambiti applicativi”, 2018.

- Bernasconi Anna, Ferragina Paolo, Luccio Fabrizio, “Elementi di crittografia”, 2015.
- Binance Academy, “Crypto & Blockchain Education”, 2020.
- Borsa Italiana, “Bitcoin, cos’è e come funziona”, 2019.
- Broggi Joshua David, “Building the first Blockchain University”, 2018.
- Buterin Vitalik, Ethereum White Paper, “A next generation smart contract & decentralized application platform”, 2014.
- Carli Francesca, “La crittografia: quando nasce, come funziona e perché è alleata della sicurezza informatica”, 2020.
- Carson Brant, Romanelli Giulio, Walsh Patricia, Zhumaev Askhat, “Blockchain beyond the hype: What is the strategic business value”, 2018.
- Chaum David, “Blind Signature for Untraceable Payments”, 1982.
- Chohan, Usman W., “The Double Spending Problem and Cryptocurrencies”, 2017.
- Croman K., “On Scaling Decentralized Blockchains”, 2016.
- Dai Wei, “B-money, an anonymous, distributed, electronic cash system”, 1998.
- De Maldè Mirko, “Il ruolo della tecnologia blockchain per combattere la pandemia da COVID-19”, 2020.
- Del Fungo Marco, “Blockchain ed energy sharing: una rivoluzione nel campo dell’energia”, 2018.

- Deloitte, Deloitte's 2020 Global Blockchain Survey, 2020.
- Diamanti Giancarlo, "Come integrare la Blockchain nel mondo dello sport", 2018.
- Dinh T.N., Thai M.T., "AI and Blockchain: A Disruptive Integration", Computer, Vol. 51 No. 9, pp. 48-53, 2018.
- Dong He, "IMF staff discussion note: Virtual Currency and Beyond: initial considerations", Gennaio 2016.
- Drescher D., "Blockchain Basics: A Non-Technical Introduction in 25 Steps", Apress, 2017.
- Du W. D., Pan S. L., Leidner D. E., Ying W., "Affordances, experimentation and actualization of FinTech: A Blockchain implementation study", Journal of Strategic Information Systems, 2018.
- Enisa, "Distributed Ledger Technology & Cybersecurity: Improving information security in the financial sector", 2016.
- EY, "Blockchain Technology as a Platform for Digitization. Implications for the Insurance Industry", 2015.
- Faioli Michele, "Con la Blockchain migliorano politiche del lavoro e previdenza", SOLE24ORE, 2018.
- Faioli Michele, Petrilli Emanuele, Faioli Donato, "Blockchain, contratti e lavoro. La ri-rivoluzione digitale nel mondo produttivo e nelle PA", 2019.
- Ferrari R., "L'Era del Fintech", Franco Angeli, 2016.

- Giddens Anthony, “Le conseguenze della modernità. Fiducia e rischio, sicurezza e pericolo”, 1994.
- Gipp B., Meuschke N., Gernandt A., “Decentralized Trusted Timestamping using the Crypto Currency Bitcoin”, 2015.
- Griffey Jason, “The what, how, and why of blockchain for libraries”, 2016.
- Hartman Joel, “Cryptocurrency & Blockchain: how to generate passive income with your blockchain wallet”, 2019.
- Hileman, Rauchs, “Global Blockchain Benchmarking Study”, 2017.
- Khurshid A., “Applying blockchain technology to address the crisis of trust during the COVID-19 pandemic”, JMIR medical informatics, 2020.
- Kiviat T. L., “Beyond bitcoin: Issues in regulating blockchain transactions”, Duke Law Journal, 65, pp. 569-698, 2014.
- Lee Kuo Chuen D., Deng R. H., “Handbook of blockchain, digital finance and inclusion – volume 2”, Elsevier, 2018.
- Marchesoni Eloisa, “E-Voting e blockchain, sì o no: i casi internazionali”, 2017.
- Mariotti Ilaria, Beria Paolo, Laurino Antonio, Università degli Studi di Trieste, “Car sharing peer-to-peer: un’analisi empirica sulla città di Milano”, 2013.
- Maslova Natalia, “Blockchain: disruption and opportunity”, 2018.

- Miles Raymond E., Snow Charles C., “Causes of Failure in Network Organizations”, 1992.
- Morelli Claudia, “Come scrivere uno smart contract”, 2019.
- Morkunas Vida J., Paschen Jeannette, Boon Edward, “How blockchain technologies impact your business model”, Business Horizons, vol. 62, issue 3, 295-306, 2019.
- Morkunas Vida J., Paschen Jeannette, Boon Edward, “How blockchain technologies impact your business model”, Business Horizons, 2019.
- Morriello Rossana, “Blockchain, intelligenza artificiale e internet delle cose in biblioteca”, 2019.
- Nakamoto S., “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008.
- Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S., “Bitcoin and cryptocurrency technologies: A comprehensive introduction”, Princeton University Press, 2016.
- Neudecker Till, Hartenstein Hannes, “Network Layer Aspects of Permissionless Blockchains”, 2019.
- Nexo, “Nexo: The World’s First Instant Crypto-baked Loans”, White Paper, 2018.
- Nicotra Massimiliano, “ICO Initial Coin Offering: una ricostruzione giuridica del fenomeno”, 2019.

- Nicotra Massimiliano, “Il regime giuridico delle ICOs. Analisi comparata e prospettive regolatorie italiane”, 2019.
- Nicotra Massimiliano, Sarzana di S. Ippolito Fulvio, “Diritto della blockchain, intelligenza artificiale e IoT”, 2018.
- Nowiński W., Kozma M., “How can Blockchain technology disrupt the existing business models?”, Entrepreneurial Business and Economics Review, Vol. 5 No. 3, pp. 173–188, 2017.
- Osservatorio Blockchain & Distributed Ledger, “Blockchain & Distributed Ledger: unlocking the potential of Internet of Value”, 2020.
- Pagano Marilù, “Blockchain. Cyberwar e strumenti di intelligence”, 2017.
- Parola Lorenzo, Merati Paola, Pavotti Giacomo, “Blockchain e smart contract: questioni giuridiche aperte”, 2018.
- Pearce, “The Company Mission As a Strategic Tool”, 1982.
- Penard W., Van Werkhoven T., “On the Secure Hash Algorithm family”, 2002.
- Perinetti Emanuela, “Cosa succede quando blockchain e sport industry si incontrano”, 2018.
- Perugini Maria Letizia, “Distributed ledger technologies e sistemi di Blockchain: digital currency, smart contract e altre applicazioni”, 2018.
- Pezzuto Antonio, “Brevi note sulle Initial Coin Offerings (ICOs)”, Studio Legale Tidona e Associati, Rivista di diritto Bancario e Finanziario, 2019.

- Pittaluga Francesco, “Elementi accessori del contratto: la condizione”, 2005.
- Portale Valeria, Blockchain & Distributed Ledger, “Initial Coin Offer (ICO) e Token”, 2019.
- Porter Michael E., “Competitive Advantage, Agglomeration Economies, and Regional Policy”, 1996.
- PwC, PwC Global Blockchain Survey, 2018.
- Rivest R. L., Shamir A., Adleman L., “A method for obtaining digital signatures and public-key cryptosystems”, 1978.
- Sayeed S., Marco-Gisbert H., “Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack”, University of the West of Scotland, 2019.
- Singh N., “Top 7 Blockchain Business Models That You Should Know About”, 2018.
- Soldavini Pierangelo, “Bitcoin in caduta libera perde il 30% in una settimana: le tre ragioni del crollo”, SOLE24ORE, 2018.
- Sottocorona Chiara, “Blockchain, che cos’è e a cosa serve: dal supermercato alle polizze, come funziona nella vita quotidiana”, 2019.
- Strategy Innovation Forum, “Gli impatti di IA e di Blockchain sui modelli di business”, 2020.

- Studio Legale Saglietti-Bianco, “Le nuove sfide della proprietà intellettuale: Blockchain e Smart Contract”, 2019.
- Szabo Nick, “Formalizing and Securing Relationships on Public Networks”, 1997.
- Szabo Nick, “Secure Property Titles with Owner Authority”, 1998.
- Tapscott, D., Tapscott, A., “The Impact of the Blockchain Goes Beyond Financial Services”, Harvard Business Review, 2016.
- Tenga Federico, “The DAO e possibili fork di Ethereum”, 2016.
- Torchiani Gianluigi, “European Blockchain Service Infrastructure (EBSI), che cos’è e quali sono i vantaggi”, 2019.
- Treiblmaier H., “The impact of the Blockchain on the supply chain: a theory-based research framework and a call for action”, Supply Chain Management, Vol. 23 No. 6, pp.545–559, 2018.
- Treiblmaier H., “The impact of the blockchain on the supply chain: a theory-based research framework and a call for action”, 2018.
- Tumasjan A., Beutel T., “Blockchain-Based Decentralized Business Models in the Sharing Economy: A Technology Adoption Perspective”, Business Transformation through Blockchain, pp. 77–120, 2019.
- Università degli Studi di Cagliari, “Certificati di laurea, autenticità garantita con la Blockchain”, 2018.

- Università degli Studi di Milano Bicocca, “Bicocca rilascia le prime certificazioni di laurea Blockcerts”, 2019.
- Velcich Franco, “Mobi, il consorzio nato per studiare come la blockchain rivoluzionerà l’industria dell’auto”, 2018.

SITOGRAFIA

- www.academy.binance.com.
- www.bitoin.org.
- www.blockchain.com.
- www.blockchain4innovation.it.
- www.blocksafetech.com.
- www.blog.osservatori.net.
- www.borsaitaliana.it.
- www.cbinsights.com.
- www.consob.it.
- www.etherevolution.eu.
- www.guardacome.com.
- www.nicom672.wordpress.com.
- www.portagolioelettronicomigliore.com.